[redacted] (OCA) (FBI) b6 b7C

**From:** KALISCH, ELENI P. (OCA) (FBI)
**Sent:** Thursday, March 17, 2005 12:07 PM
**To:** FBI_SAC's; FBI_ADs and EADs
**Subject:** Patriot Act Examples
**Importance:** High



**UNCLASSIFIED**
**NON-RECORD**

All:

As the Director mentioned at the SAC Conference earlier this week, 16 provisions of the Patriot Act are scheduled to "sunset" at the end of the year. In seeking reauthorization of these provisions, we need to provide Congress with examples of how these provisions have been helpful to us in all of our programs. The text of the Patriot Act, as well as a summary of the 16 "sunset" provisions, are located on the OCA intranet website (http://oca.fbinet.fbi) under the "Legislation of Interest" link.

**Please review these provisions and submit unclassified examples to me via e-mail no later than Friday, March 25.**

Although examples of all provisions are needed, of particular interest are examples of the following:

Sections 201 and 202 (Expanded Title III predicates)
Sections 203 and 218 (Information Sharing)
Section 206 (Roving Wiretaps)
Section 214 (FISA Pen Register and Trap/Trace)
Section 215 (Business Records)
Section 217 (Computer Hacking victims requesting law enforcement assistance)

Although not subject to sunset, Section 213 (Delayed Notice Search Warrants) remains controversial and examples of the utility of this provision are needed.

In your response, please identify a POC in your office in the event additional information is needed. Thank you for your assistance.

Eleni

**UNCLASSIFIED**

# Patriot Act Sunset Provisions

| Section | Description | Comment |
|---|---|---|
| 201 | These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), and terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B). | |
| 202 | These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to felony violations of computer fraud and abuse (18 U.S.C. § 1030). | |
| 203(b) | Authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. (Wiretap info) | |
| 203(d) | Authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. ("Catch-all" / non-wiretap or 6(e)) | |
| 204 | Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications | |

b5

| Section | Description | Comment |
| --- | --- | --- |
| 206 | Roving FISA Surveillance | |
| 207 | Extended Duration for Certain FISAs | |
| 209 | Seizure of Voice Mail with a Search Warrant | |

b5

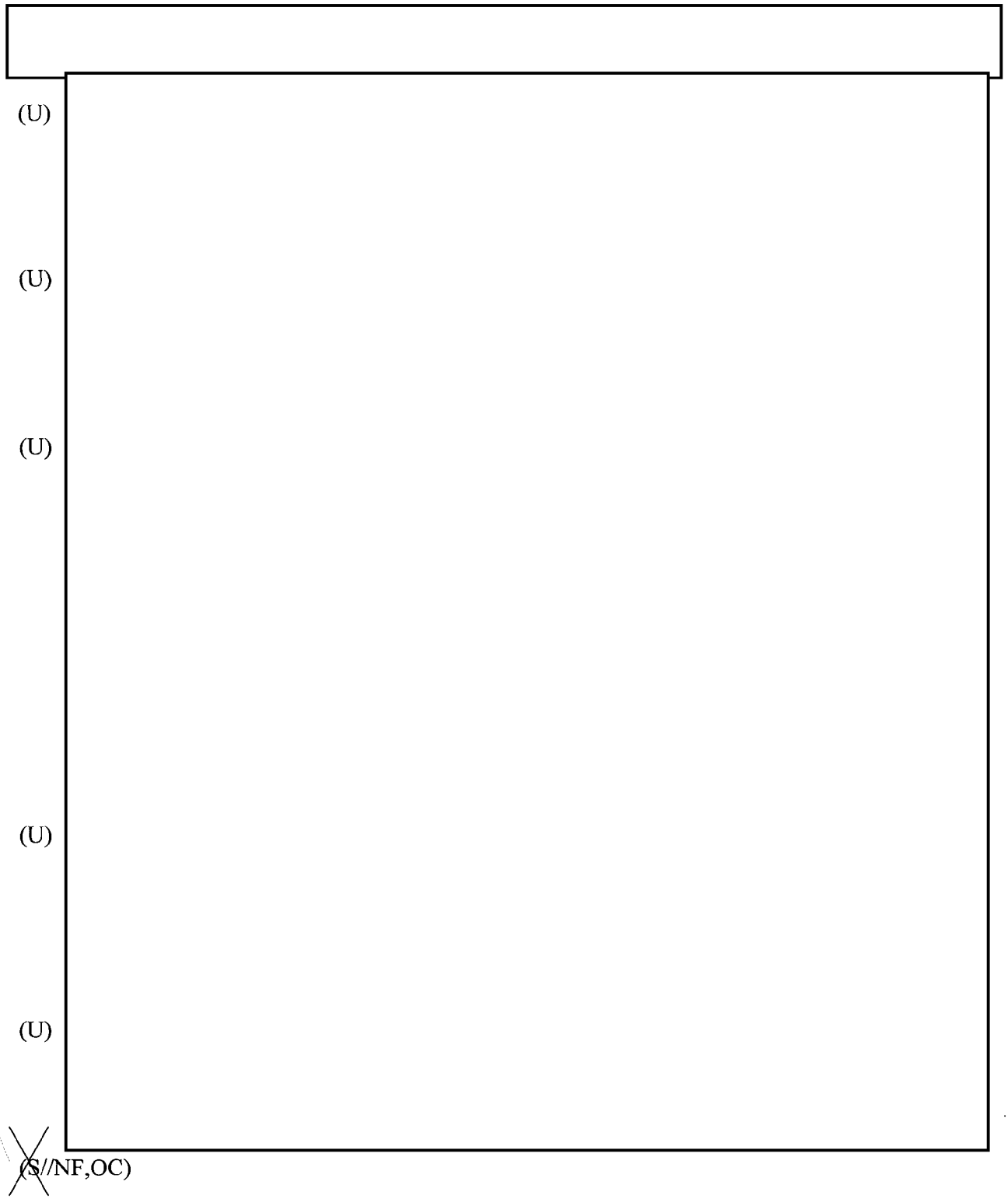
| Section | Description | Comment |
|---|---|---|
| 212 | Emergency Disclosures of E-mail & Records by ISPs | |
| 214 | FISA Pen/Trap Authority | |
| 215 | Access to Business Records under FISA | |
| 217 | Interception of Computer Trespasser Communications | |

b5

| Section | Description | Comment |
|---|---|---|
| 218 | Change in the "Primary Purpose" Standard of FISA | |
| 220 | Nationwide Search Warrants for Electronic Evidence | |
| 223 | Civil Liability for Certain Unauthorized Disclosures | |
| 225 | Immunity for Compliance with FISA Wiretap | |

b5

b5



(U)

(U)

(U)

(U)

(U)

(U)

(S//NF,OC)

(U)

(U)

(S) (U)

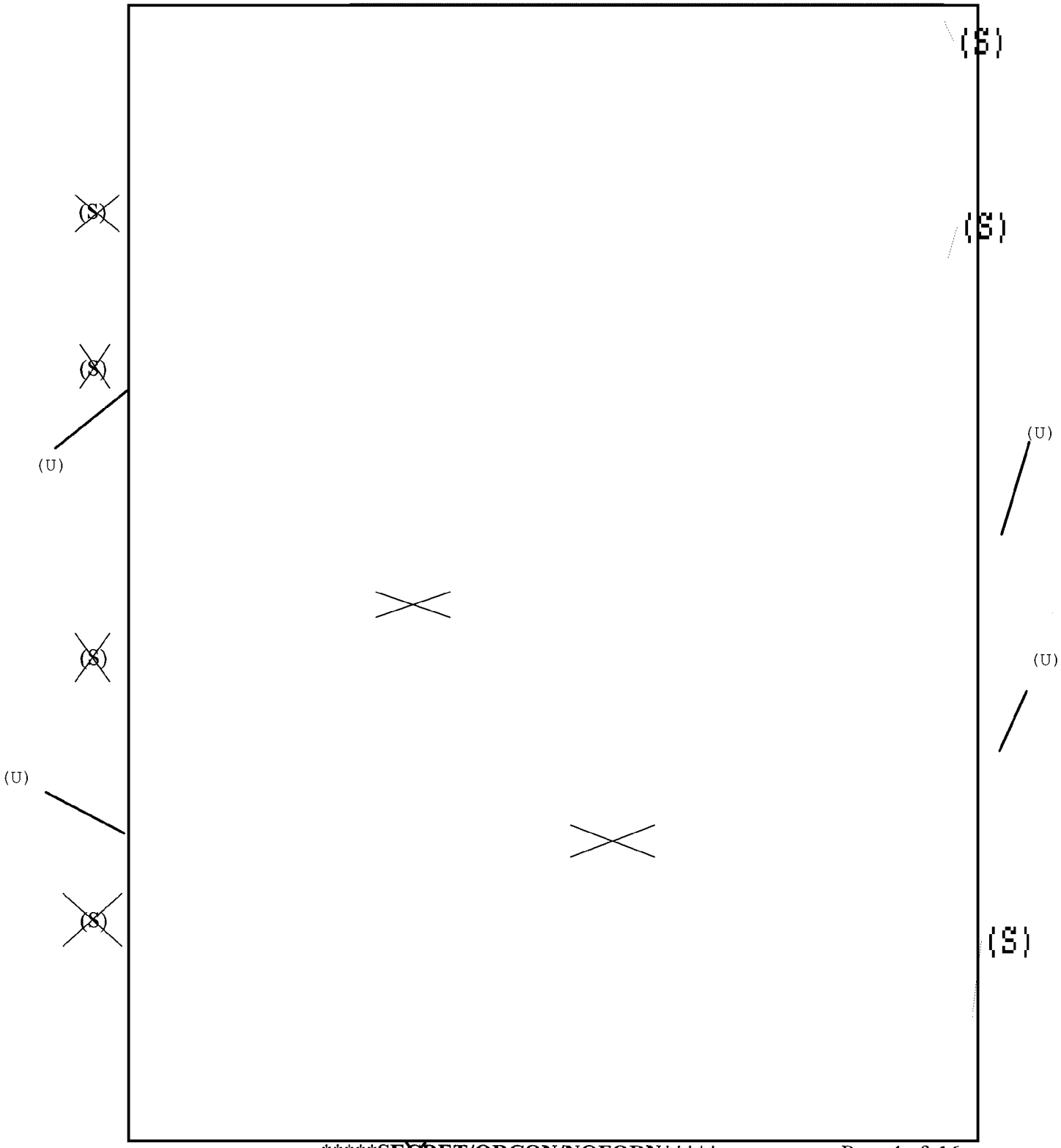
(S)

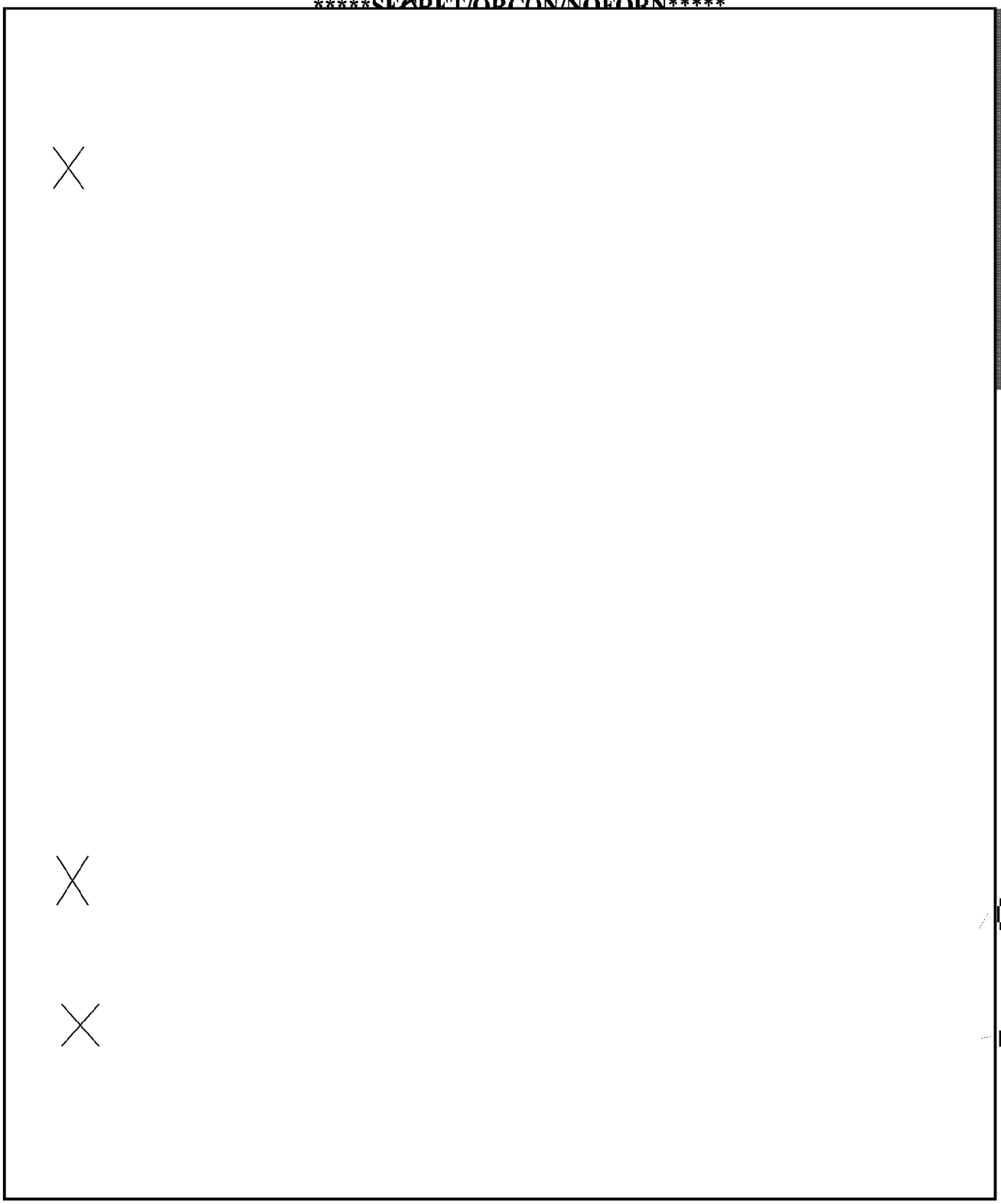
(S)

(S)

b1
b5
b6
b7A
b7C



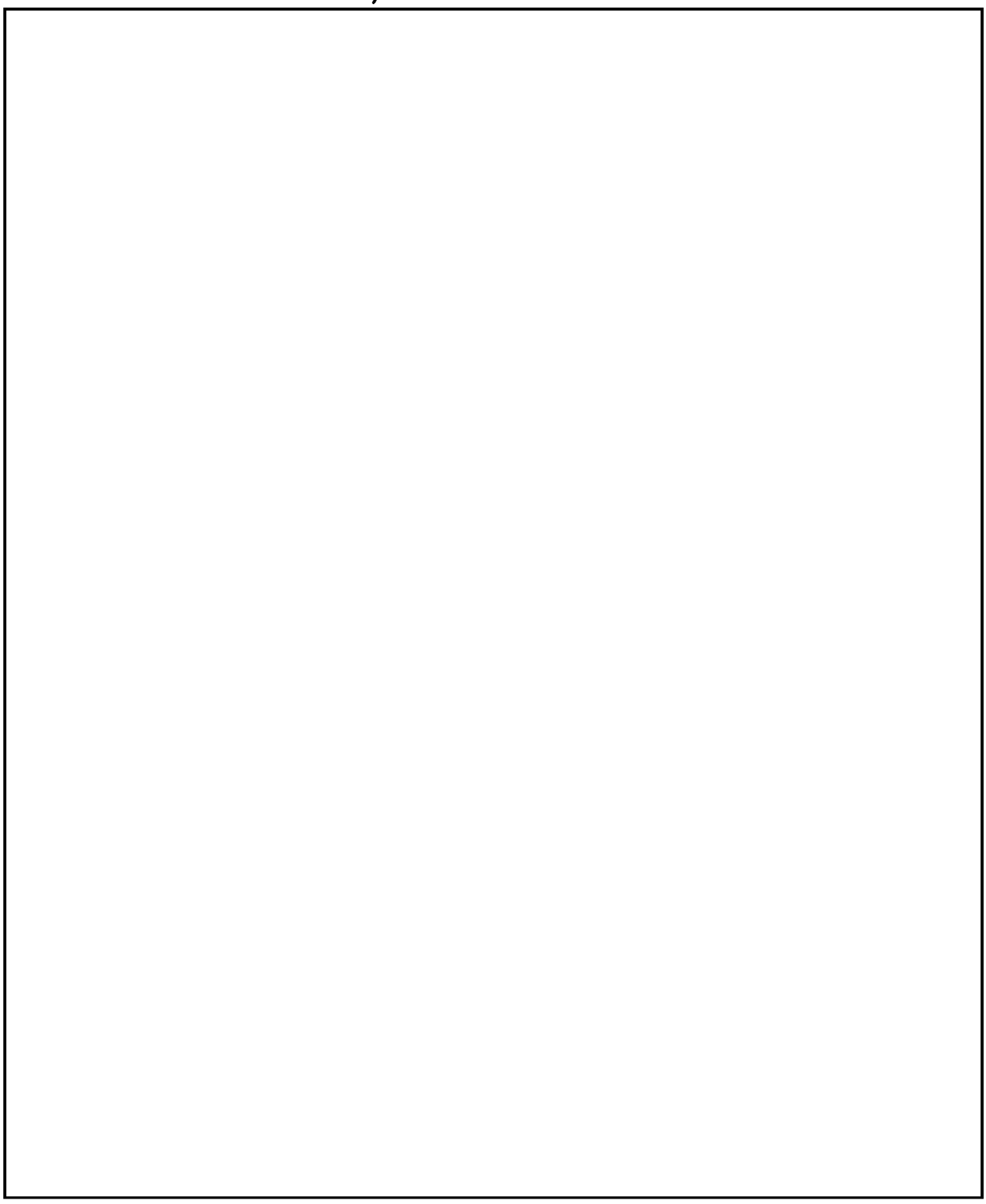


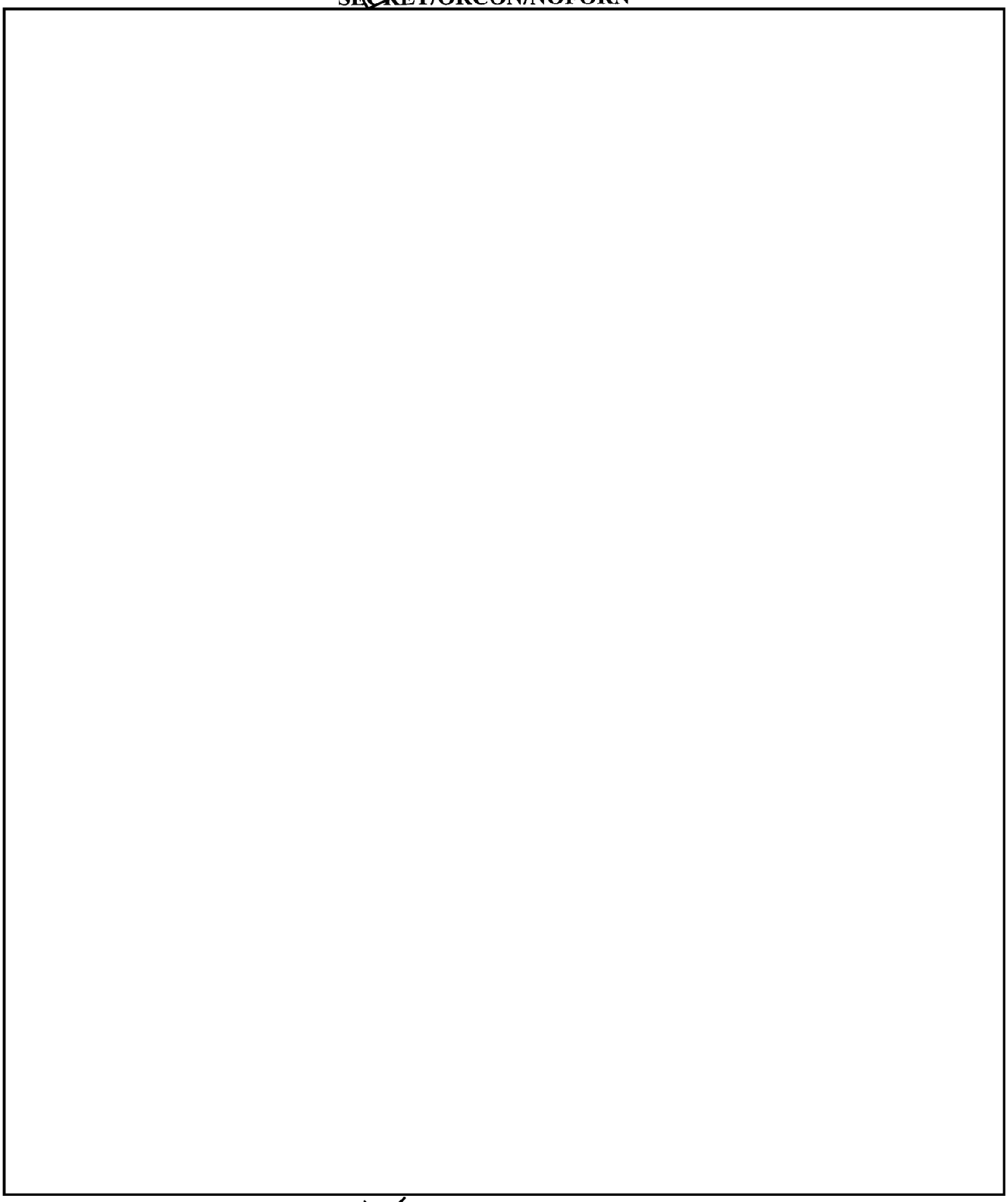


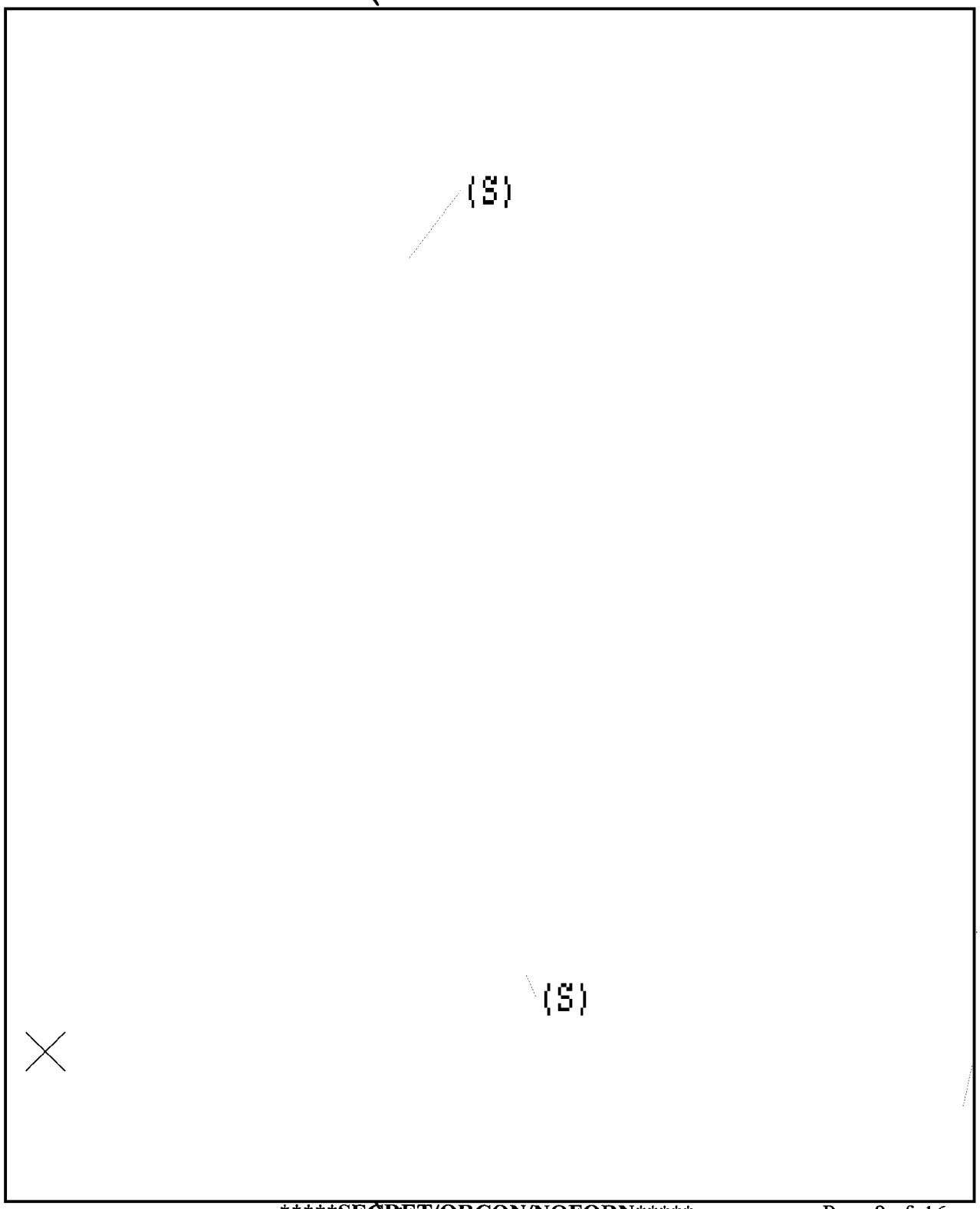
(S)

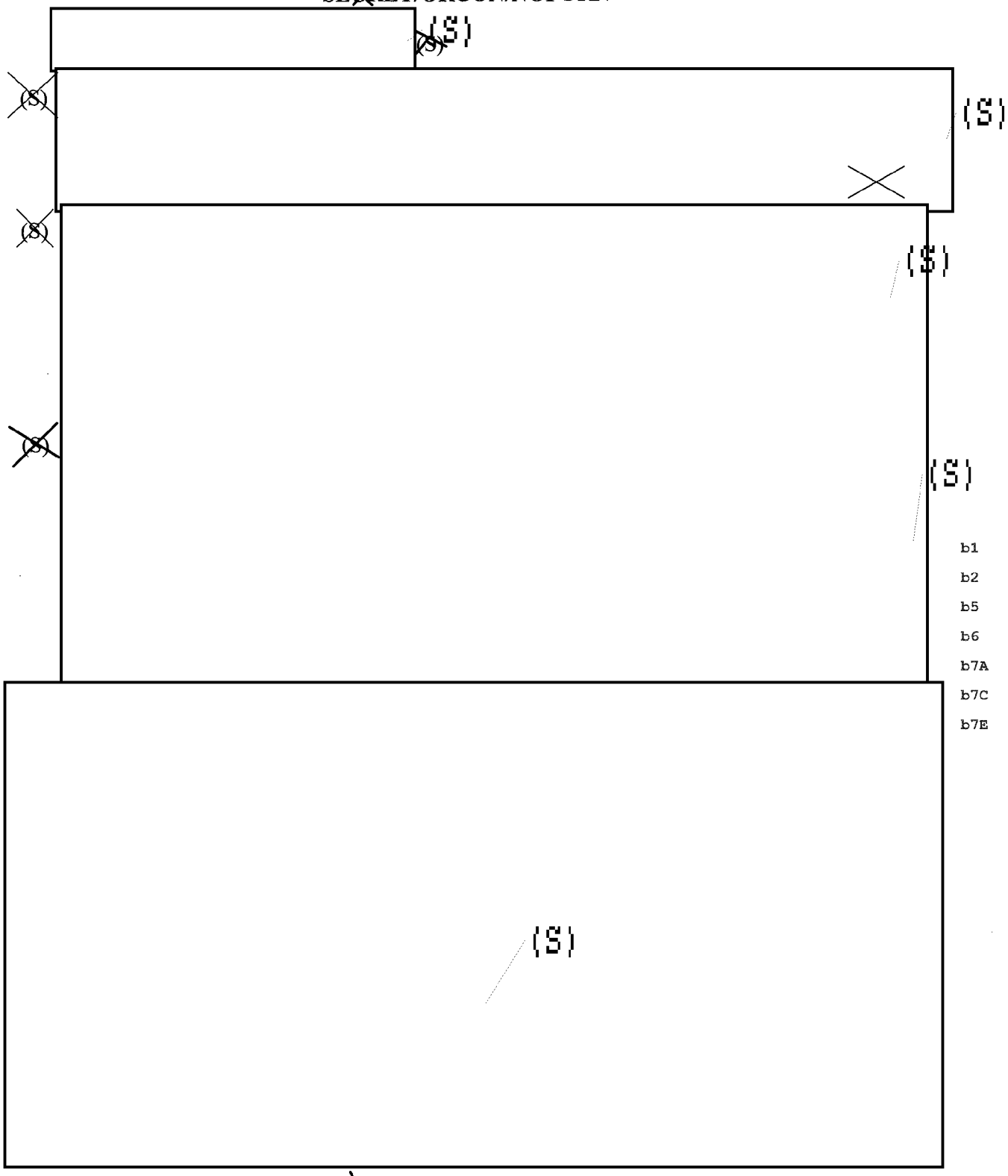
(S)

(S)

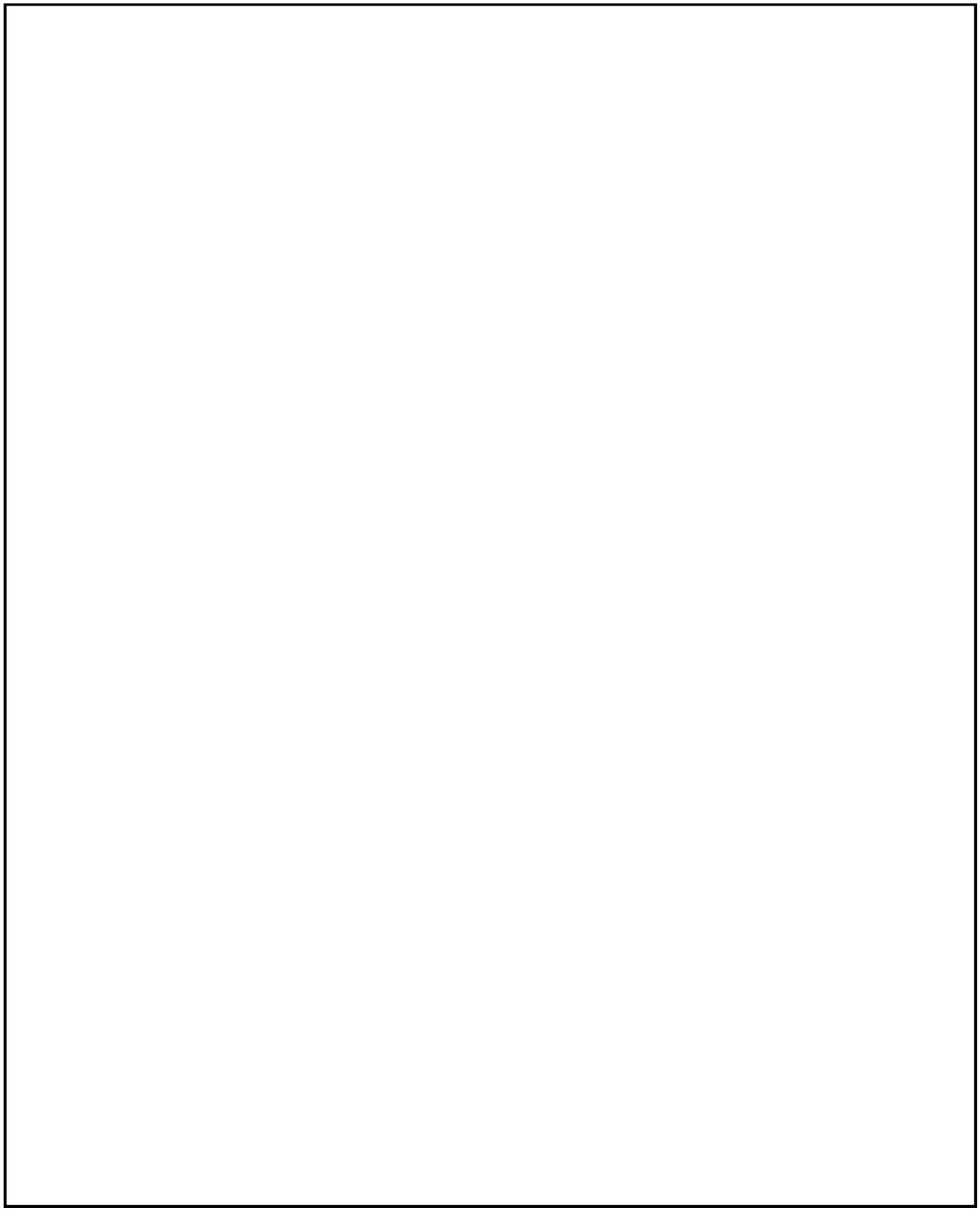


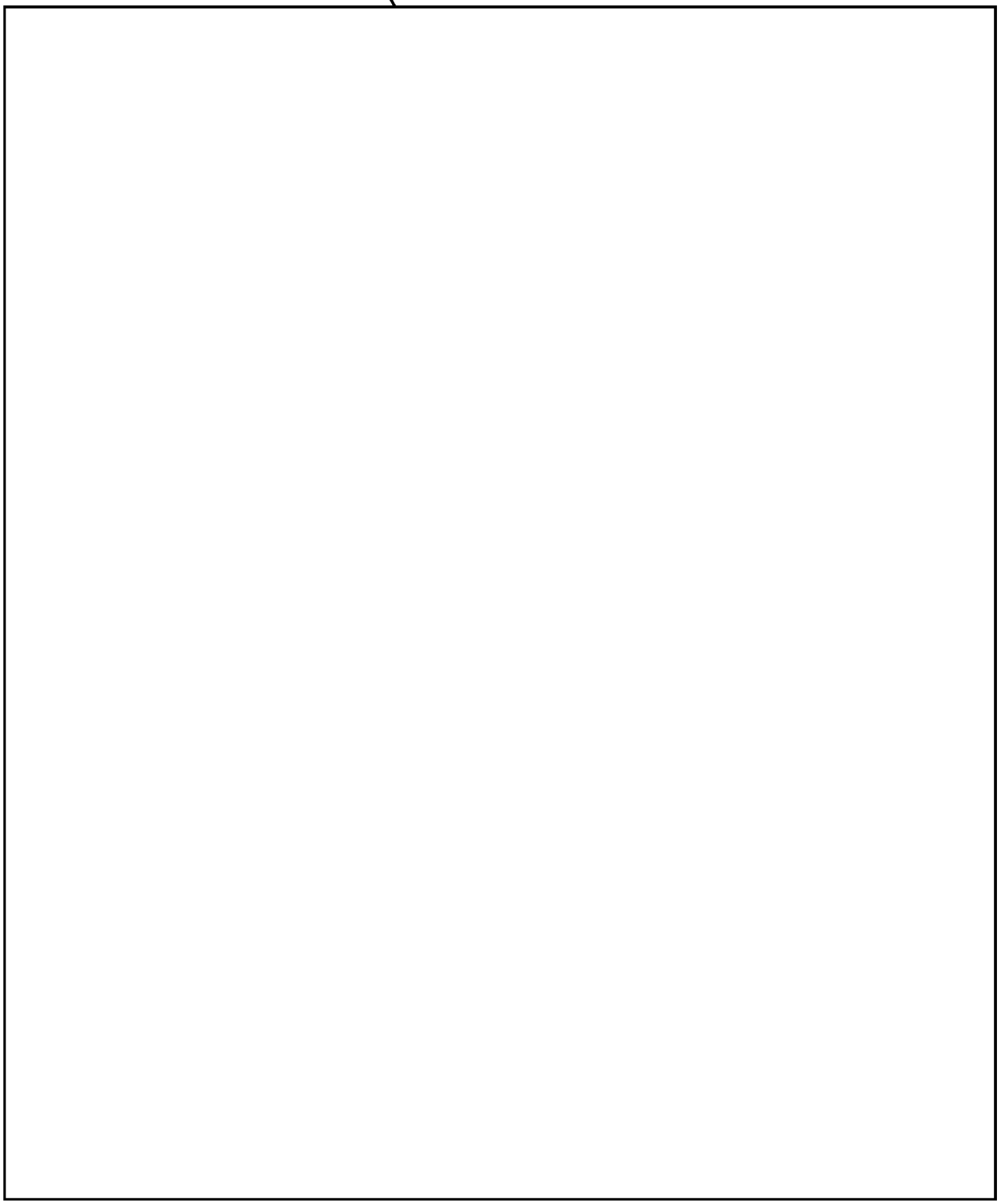



(S)
(S)
(S)




b1
b2
b5
b6
b7A
b7C
b7E





(U)

(U)

(U)

(U)

b1
b2
b5
b7A
b7D
b7E

(U)

(U)

(U)

(S)

(S)

(S)

(S)

(S)

(S//NF,OC)

(S)

b1
b2
b5
b7E

(S)

(U)

(U)

(U)

(S)

(S)

(LES)

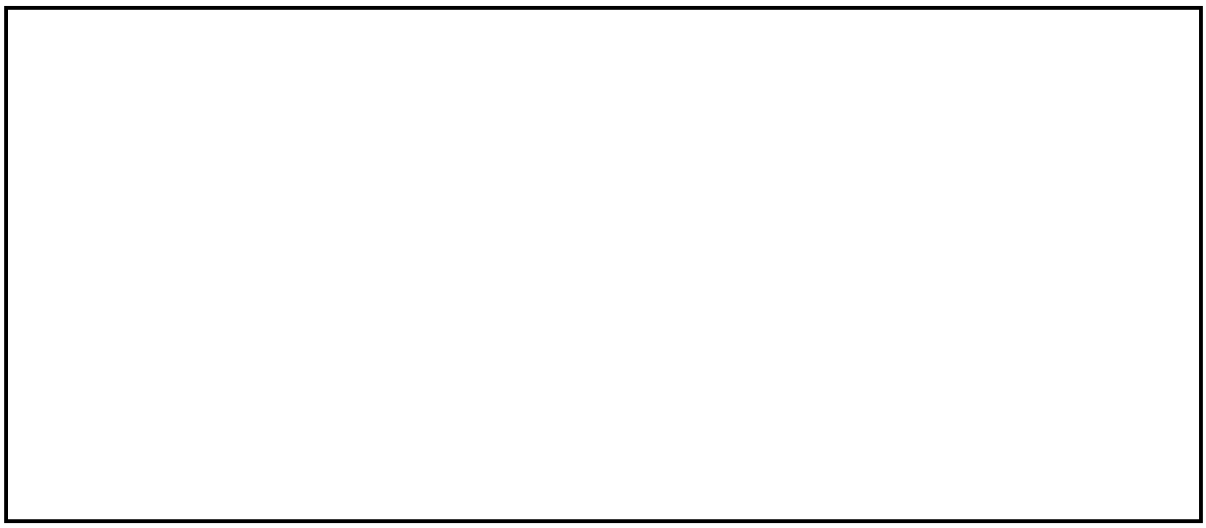
(U)

(U)

(U)

(U)

b5



**Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.**

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. (Wiretap info)

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. (Catch all - non-wiretap, non-6(e))

**EXAMPLES**

b2
b7A
b7E

b1
b2
b7E
(S)

b2
b7E

b2
b7D
b7E

(S)

b1
b2
b6
b7A
b7C
b7E

(S)

[redacted]

[redacted] initiated an investigation partially predicated upon information [redacted] b7A b6 b7C

[redacted]

Due to the significance of some of the intelligence information in cited matter an [redacted] b7A b6 b7C

[redacted] b2 b7E

[redacted] b6 b7C

[redacted]

b2 b7E

**Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications**

Prior to the Patriot Act, federal statutes governing the use of criminal investigative wiretaps stated that the interception of wire or oral communications for foreign intelligence purposes should be governed by the provisions of the Foreign Intelligence Surveillance Act (FISA), rather than Title III. This provision, however, did not refer to electronic communications. As a result, it was arguably unclear whether the interception of electronic communications, such as e-mail messages, for foreign intelligence purposes was governed by FISA or Title II (or both). Section 204 clarified the uncertainty by amending Title 18 to confirm that in foreign intelligence investigations, it is FISA, and not Title III, that governs the interception of electronic communications as well as wire and oral communications.

**EXAMPLES**

| |
|---|
| |

b2
b7A
b7E

b2
b7E

**Section 206 - Roving FISA Surveillance**

When a FISA target's actions have the effect of thwarting surveillance,

b5

DOJ has not declassified the number of requests for roving surveillance authority.

(S)

b1
b2
b7E

**Section 207 - Extended Duration for Certain FISAs**

b5

Section 207 extends the standard duration for several categories of FISA orders.

**Section 209 - Seizure of Voice Mail with a Search Warrant**

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703 (similar to e-mail). Previously, some courts had required a Title III order to obtain stored voice mail. The language in Section 209 of the Patriot Act eliminated the distinction in the definitions for "wire communication" and "electronic communication" that was relied on in a 2004 First Circuit opinion (United States v. Councilman) to minimize privacy protection for e-mail. As such, should Congress allow this provision to sunset, it may be unintentionally signaling to the First Circuit and other courts that Congress intends to reduce the privacy protection for e-mails in transit.

**EXAMPLES**

**Section 212 - Emergency Disclosures of E-mail & Records by ISPs**

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury.

**EXAMPLES**

National Science Foundation's South Pole Station

In May of 2003, the WFO Cyber Squad conducted an investigation involving the computer hacking of the National Science Foundation's South Pole Station. Utilizing the Emergency Disclosures of E-mail & Records by ISPs (section 212), the FBI was able to identify and locate the subject who had hacked into the South Pole Station's computer system and obtained access control of various systems, to include the station's life support.

Jared Bjarnason

The section was utilized by the El Paso Division in April of 2004 to arrest an individual threatening to destroy an El Paso mosque. Jared Bjarnason, an El Paso resident, sent an e-mail message to the El Paso Islamic Center on April 18, 2004. In this message, he threatened to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Agents investigating the threat utilized section 212 to expeditiously obtain information from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could harm the mosque. Absent the emergency access afforded by section 212, the Agents would probably not have been able to locate and arrest Bjarnason in time to stop him, were he to carry out his stated threats. Bjarnason pleaded guilty to sending a threatening interstate communication and making a threat against a religious property. He was sentenced to 18 months in federal prison and ordered to complete 150 hours of community service.

Scott Tyree

Section 212 of the PATRIOT Act was utilized to rescue a 13-year old girl who had been lured from her Western Pennsylvania home by a 39-year old man who she met online, and who was holding her captive at his residence in Virginia.

Scott Tyree was a 38 year old divorced 300 pound computer analyst who spent his free time trolling the internet for young teenage girls who he wanted to make his sex slave. Tyree's screen name was "master for teen slave girls."

Unbeknownst to her parents, a 13 year old Pittsburgh girl began chatting online with Tyree in December, 2001. Tyree exploited this young girl's vulnerabilities and befriended her on the internet. After a month of chatting, Tyree convinced the girl that she should come and live with him in his home in Virginia. He drove to Pennsylvania to pick her up on 01/01/2002.

On 01/02/2002, FBI Pittsburgh received a report from the Pittsburgh Bureau of Police that a 13-year old girl had disappeared from her parents' home on the previous day. FBI agents interviewed the parents and the victim's friends, one of whom reported that the victim had been talking about leaving Pittsburgh with a man she met online. Her computer was examined, but it had been wiped clean. Over the next two days, agents and police officers searched for clues to this child's whereabouts, without any luck.

A break came the evening of 01/03/2002, when the FBI received an anonymous call from a man in Florida who claimed that he had an online friend who lived in Northern Virginia who claimed that he had taken a girl from Pittsburgh to make her his sex slave. The Florida man told the FBI he saw a video, via a live web camera broadcast, of the girl. The girl was naked, and, according to the online friend, had just been beaten. The caller could not recall the screen name used by the man.

On the morning of 01/04/2002, the anonymous caller recontacted the FBI and advised that the suspect used the screen name "master for teen slave girls @ yahoo. com." FBI agents immediately tried to contact Yahoo to find out who this person was. Because Yahoo is based on California and it was the middle of the night, Pacific time, Pittsburgh agents had to contact a Yahoo Vice President at his home in California to trace this screen name. Thanks to a provision in the Patriot Act, the Yahoo Vice Present was able to provide identifying information about the screen name without a grand jury subpoena. This provision of the Patriot Act, Section 212, (18 U.S.C. § 2702(b)} allows an Internet Service Provider to immediately provide information to law enforcement in the case of an emergency involving an immediate risk of death or serious bodily injury. As a result of that provision of the Patriot Act, we were able to quickly identify Scott Tyree and find out where he lived. Agents immediately went to Tyree's residence and rescued the child victim, who was found laying nearly naked in a bed, with a collar around her neck, chained to a wall. Tyree was arrested that same day at his place of employment, Computer Associates in Virginia.

We later learned while the child victim was trapped in Tyree's Virginia home for 4 days, that he treated her as his sex slave, physically and sexually abusing her. The child victim was collared and kept chained in Tyree's bedroom or chained in a "dungeon" in his basement, where he kept hundreds of sado masochistic devices.

Tyree eventually pled guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor (18 U.S.C. §§ 2423(b) and 2251(a)) and was thereafter sentenced to a term of 235 months imprisonment.

**Section 214 - FISA Pen/Trap Authority**

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

**EXAMPLES**

The total number of orders by the Foreign Intelligence Surveillance Court authorizing the installation and use of pen registers and trap and trace devices for the period of October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

DOJ has not declassified the number of requests for FISA pen register / trap trace authority.

(S)

b1

(S)

(S)

b2
b7E

**Section 215 - Access to Business Records under FISA**

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] to include "any tangible things (including books, records, papers, documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

**EXAMPLES**

The total number of orders approved by the Foreign Intelligence Surveillance Court for access to certain business records for foreign intelligence purposes under this provision from October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

The number of such order issued to libraries and/or booksellers from October 26, 2001 through March 31, 2005 has been declassified. The total number is _____.

The categories of information that have been sought to date in orders for the production of tangible things under Section 215 of the Act, specifically:

1) [redacted]
2)
3)
4)
5)

b2
b7E

DOJ has not declassified the number of requests for FISA business record orders.

**Section 217 - Interception of Computer Trespasser Communications**

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

**EXAMPLES**

The hacker trespasser exception has been an important tool for law enforcement to obtain evidence based on the consent of the victim. A diverse array of examples from the Cyber criminal investigations include (a) the FBI's investigation of hackers who took over a local government server in order to collect credit card and drivers license numbers of victims of a major identity theft phishing scam; (b) the FBI's investigation of hackers who broke into the network of a major Trust, and whose server then became the storage facility for pirated software, movies, and video games; and (c) the joint investigation by the FBI and the [redacted] b7D [redacted] into a hacker who broke into a router used by the United States Supreme Court.

## Section 218 - Change in the "Primary Purpose" Standard of FISA

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal investigators or prosecutors without putting their FISAs at risk.

**EXAMPLES**

As stated above, FBI field offices overwhelmingly herald the information sharing provisions as the most important provisions in the USA Patriot Act. Section 218 is an essential component to these changes. This provision allows prosecutors to be involved in the earliest phases of an international terrorism investigation without jeopardizing the use of the FISA technique. AUSAs are often co-located with the JTTFs and are able to provide immediate input regarding the use of criminal charges to stop terrorist activity, including the prevention of terrorist attacks.

PIJ [redacted] b6 b7C

A limited amount of FISA-derived information was passed over "the wall" prior to the passage of the Patriot Act for use in a pending criminal investigation of the worldwide leadership of the Palestinian Islamic Jihad (PIJ), a designated foreign terrorist organization. Prior to the passage of the Patriot Act, an indictment was being prepared, based in part on this FISA-derived information. When the "wall" came down, voluminous information was passed to the criminal investigators and prosecutors giving them a much clearer understanding of the case. As a result, a superseding indictment was filed on the case on [redacted]

Prior to the passage of the Patriot Act and prior to "the wall" coming down, [redacted] summaries and [redacted] were selected by intelligence investigators and passed "over the wall" to the criminal investigators assigned to this case. This information was later declassified and utilized in preparing an initial RICO indictment, which was returned on February 19, 2003. After "the wall" came down, the criminal investigators had the opportunity to review all information derived from a series of [redacted] that were in operation over a period of approximately nine years. [redacted] b2 b7E b6 b7C Consequently, new overt acts were developed, existing overt acts were enhanced, and the prosecutive theory of the case became stronger. A superseding indictment was returned on [redacted] which added additional charges and overt acts, streamlined the prosecutive theory, and added another subject who was previously named as an unindicted co-conspirator.

[redacted] investigation and RICO prosecution as a new method of attacking terrorism following the passage of the Patriot Act. The jury trial of [redacted] and others is set to begin on 05/16/2005 in [redacted] Florida.

b6
b7C
b2
b7E

**Section 220 - Nationwide Search Warrants for Electronic Evidence**

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

**EXAMPLES**

INNOCENT IMAGES (S)

Baltimore has utilized th[redacted]imes in connection with its Innocent Images investigation. Baltimore's experience in the use of the nationwide search warrants to obtain e-mail from ISPs has shown that they significantly reduce the time it takes to obtain contents of e-mail accounts, and results in a much more efficient use of agent investigative resources. This reduction in time can allow us to obtain information that would otherwise be lost because of the short amount of time some ISPs maintain customer data. It is foreseeable that the time saved obtaining information through the use of nationwide search warrants could have other benefits. While we can not state with certainty that up to this point the use of a nationwide search warrant definitely prevented an act of child sexual exploitation, because of the reduction in time it takes to obtain e-mail information through the use of a nationwide warrant, it is very conceivable that the use of a nationwide warrant in connection with the Innocent Images investigation could prevent such an act of child exploitation at some point in the future. b1

Scott Tyree (Also example of §212)

Section 220 of the PATRIOT Act was utilized to rescue a 13-year old girl who had been lured from her Western Pennsylvania home by a 39-year old man who she met online, and who was holding her captive at his residence in Virginia.

Scott Tyree was a 38 year old divorced 300 pound computer analyst who spent his free time trolling the internet for young teenage girls who he wanted to make his sex slave. Tyree's screen name was "master for teen slave girls."

Unbeknownst to her parents, a 13 year old Pittsburgh girl began chatting online with Tyree in December, 2001. Tyree exploited this young girl's vulnerabilities and befriended her on the internet. After a month of chatting, Tyree convinced the girl that she should come and live with him in his home in Virginia. He drove to Pennsylvania to pick her up on 01/01/2002.

On 01/02/2002, FBI Pittsburgh received a report from the Pittsburgh Bureau of Police that a 13-year old girl had disappeared from her parents' home on the previous day. FBI agents interviewed the parents and the victim's friends, one of whom reported that the victim had been talking about leaving Pittsburgh with a man she met online. Her computer was examined, but it had been wiped clean. Over the next two days, agents and police officers searched for clues to this child's whereabouts, without any luck.

A break came the evening of 01/03/2002, when the FBI received an anonymous call from a man in Florida who claimed that he had an online friend who lived in Northern Virginia who claimed that he had taken a girl from Pittsburgh to make her his sex slave. The Florida man told the FBI he saw a video, via a live web camera broadcast, of the girl. The girl was naked, and, according to the online friend, had just been beaten. The caller could not recall the screen name used by the man.

On the morning of 01/04/2002, the anonymous caller recontacted the FBI and advised that the suspect used the screen name "master for teen slave girls @ yahoo. com." FBI agents immediately tried to contact Yahoo to find out who this person was. Because Yahoo is based on California and it was the middle of the night, Pacific time, Pittsburgh agents had to contact a Yahoo Vice President at his home in California to trace this screen name. Section 220 was used to obtain search warrants for the internet service providers of Tyree and the child victim.

Agents rescued the child victim, who was found laying nearly naked in a bed, with a collar around her neck, chained to a wall. Tyree was arrested that same day at his place of employment, Computer Associates in Virginia. We later learned while the child victim was trapped in Tyree's Virginia home for 4 days, that he treated her as his sex slave, physically and sexually abusing her. The child victim was collared and kept chained in Tyree's bedroom or chained in a "dungeon" in his basement, where he kept hundreds of sado masochistic devices.

Tyree eventually pled guilty to charges of travel with intent to engage in sexual activity with a minor and sexual exploitation of a minor (18 U.S.C. §§ 2423(b) and 2251(a)) and was thereafter sentenced to a term of 235 months imprisonment.

## Section 223 - Civil Liability for Certain Unauthorized Disclosures 

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

## EXAMPLES

**Section 225 - Immunity for Compliance with FISA Wiretap**

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent or a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers, such as telephone companies or Internet service providers, to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISC without delay.

**EXAMPLES**

An FBI Special Agent was able to convince an [redacted] to assist in the installation of technical equipment [redacted] pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order. The target is an espionage subject. The device has allowed the FBI to track the path of the subject [redacted] This information has been used to understand the subject's routines and his contacts.

b2
b7E

## Section 213 - Delayed Notice Search Warrants

Pursuant to section 213, prosecutors can seek a judge's approval to delay notification by making a showing that if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:

1. notification would reasonably endanger the life or physical safety of an individual;
2. notification would reasonably be expected to cause flight from prosecution;
3. notification would reasonably be expected to result in destruction of, or tampering with, evidence;
4. notification would reasonably result in intimidation of potential witnesses; or
5. notification would reasonably be expected to cause serious jeopardy to an investigation or unduly delay a trial.

**EXAMPLES**

b1
b2
b6
b7A
b7C
b7E

Several offices have reported the use of the delayed notice provision. The circumstances cited most frequently in these investigations are that notification would reasonably be expected to result in destruction of, or tampering with, evidence and notification would reasonably be expected to cause serious jeopardy to an investigation.

[redacted] (S)

[redacted] (S)

(S)

b1
b2
b6
b7A
b7C
b7E

[redacted]

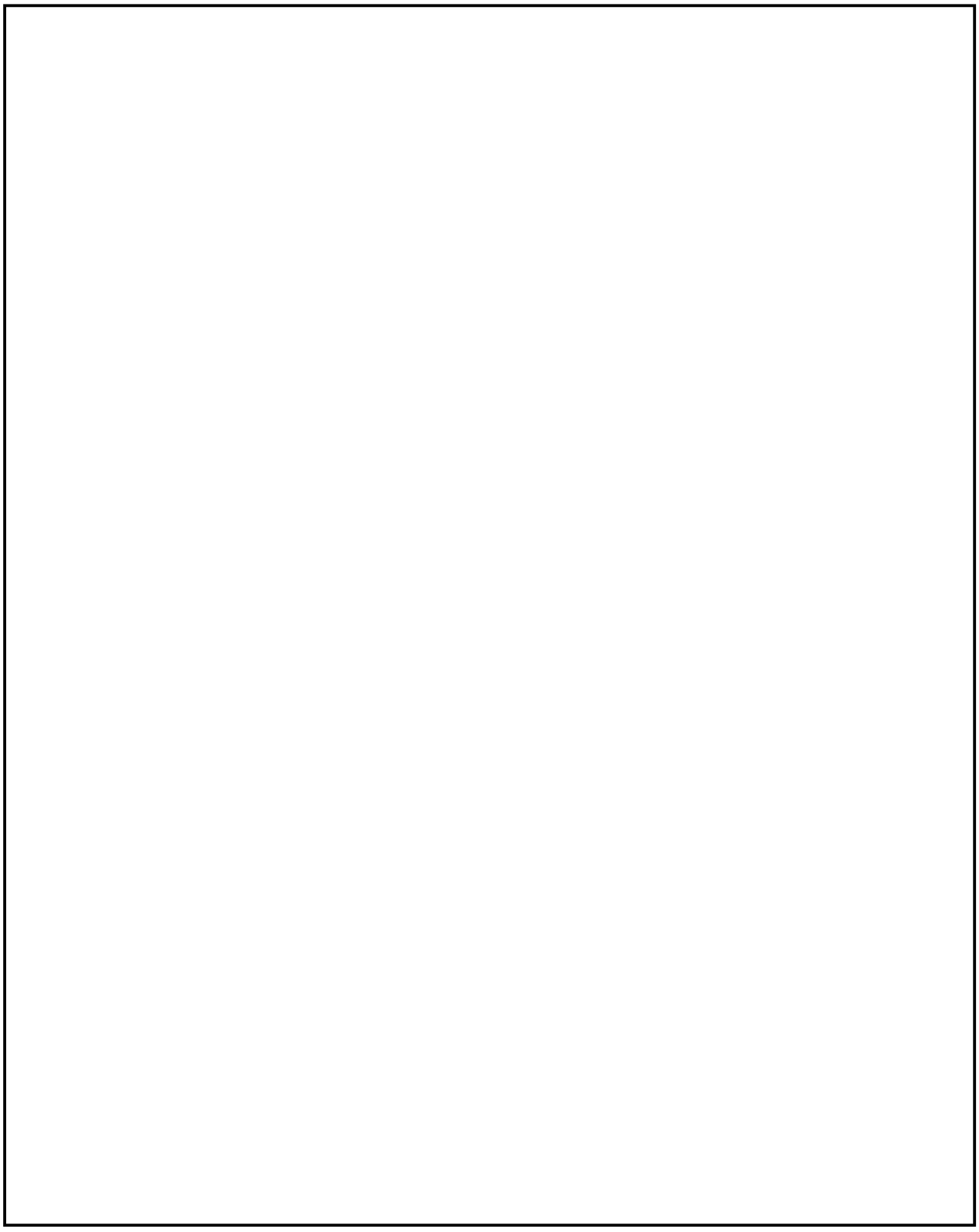
(S)

[redacted]

(S)

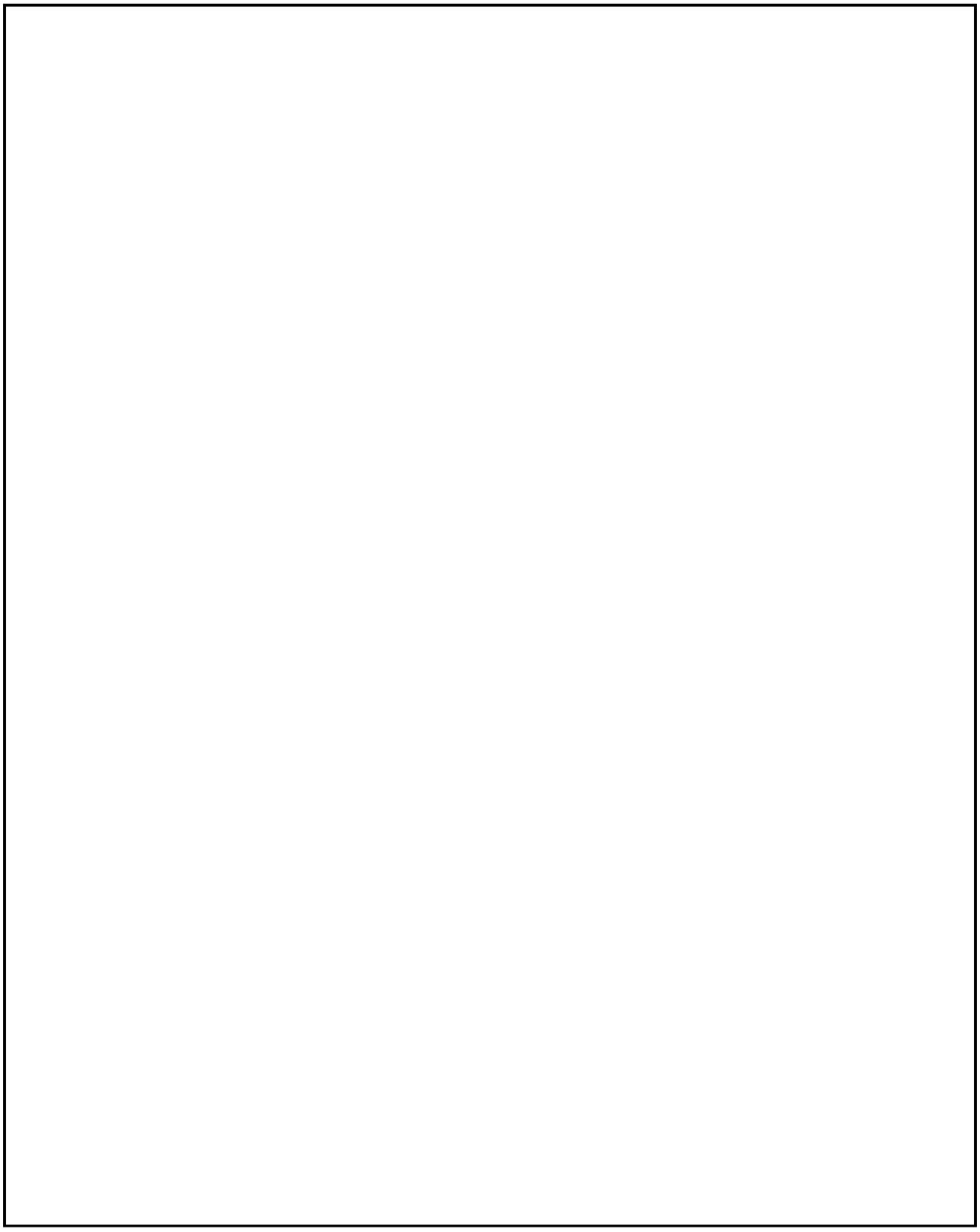
b1
b2
b6
b7A
b7C
b7E

(S)

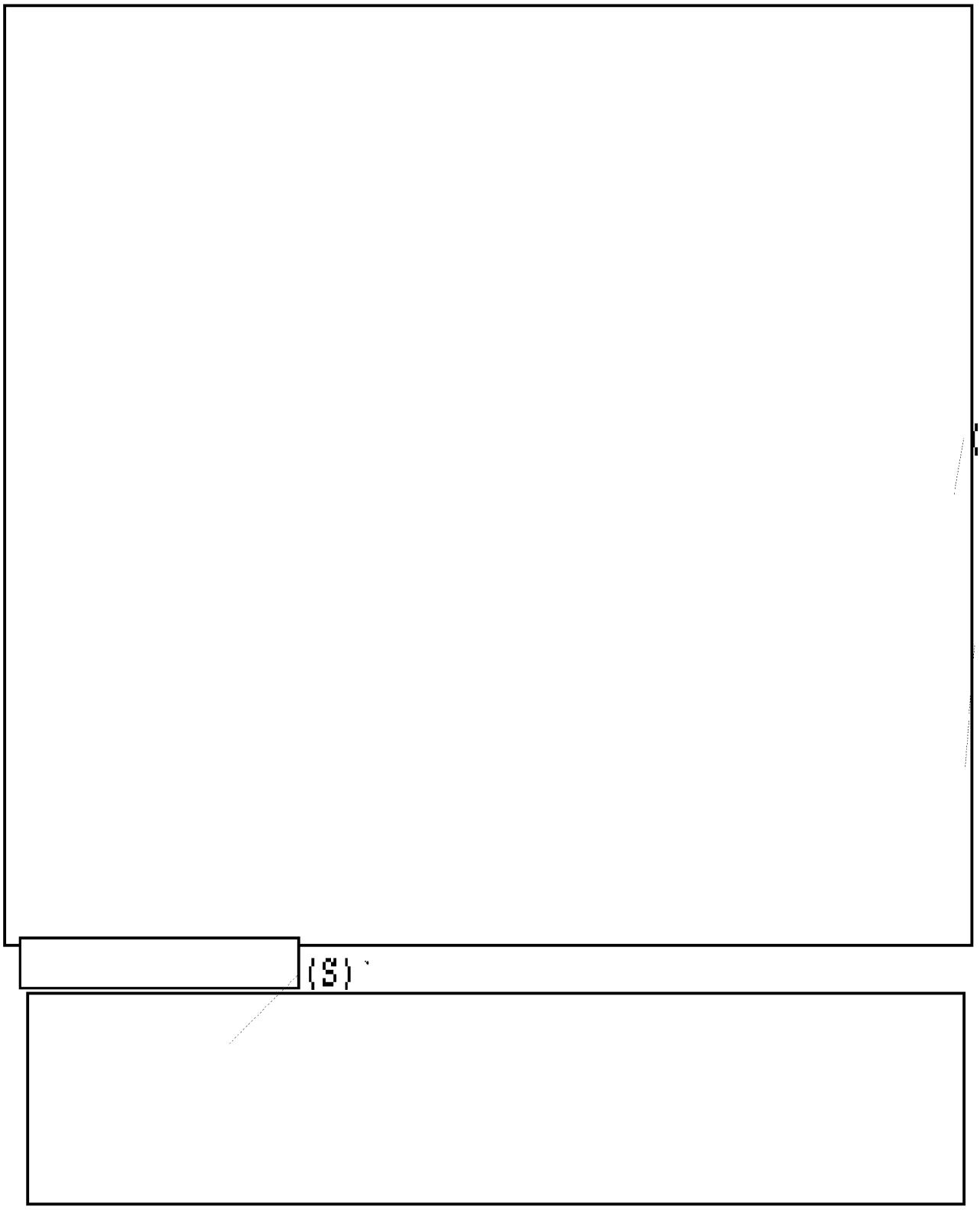


b2
b6
b7A
b7C
b7D
b7E

b6
b7A
b7C



b1
b2
b7E



(S)

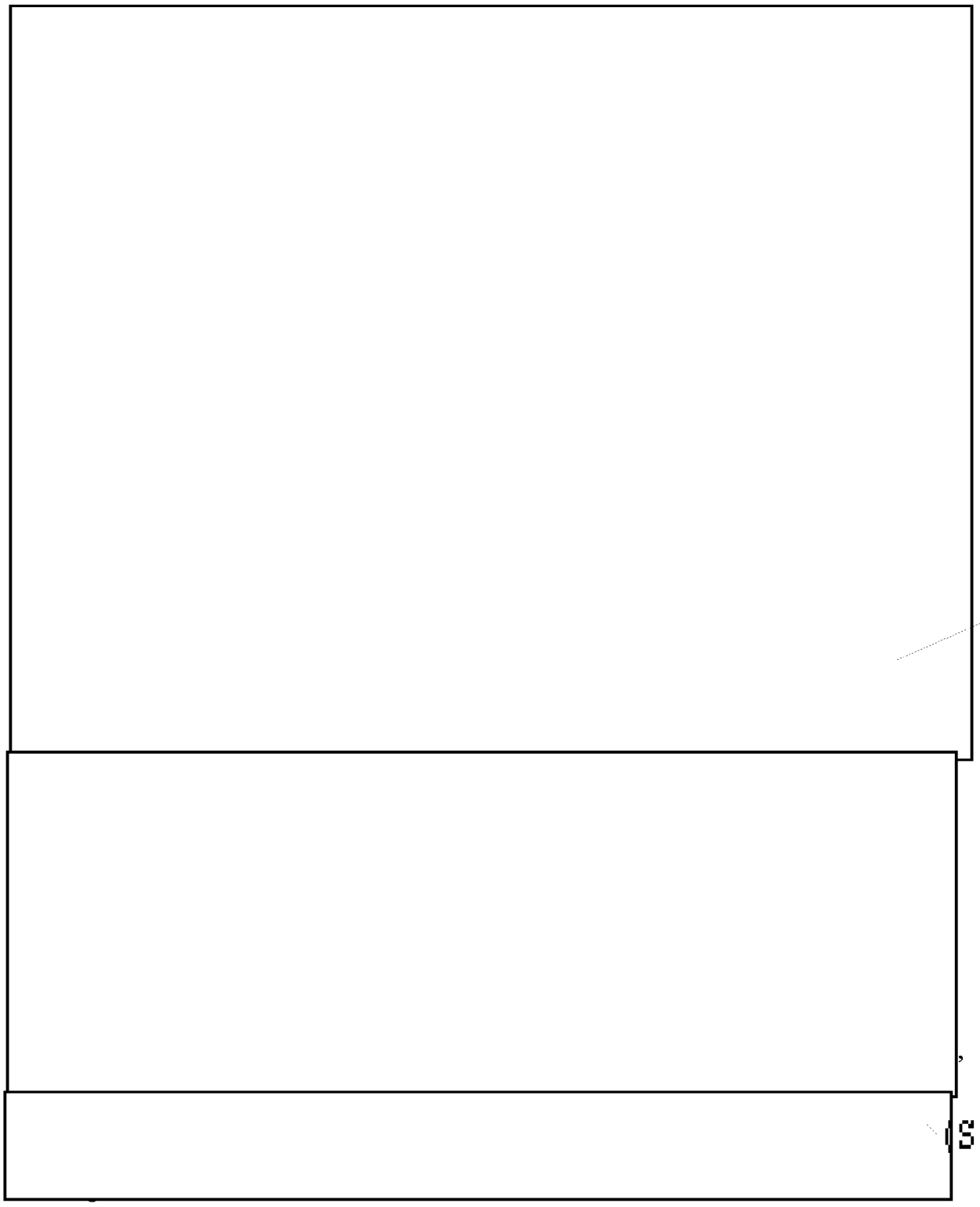
(S)

(S)



b1
b2
b7A

b2
b6
b7A
b7C

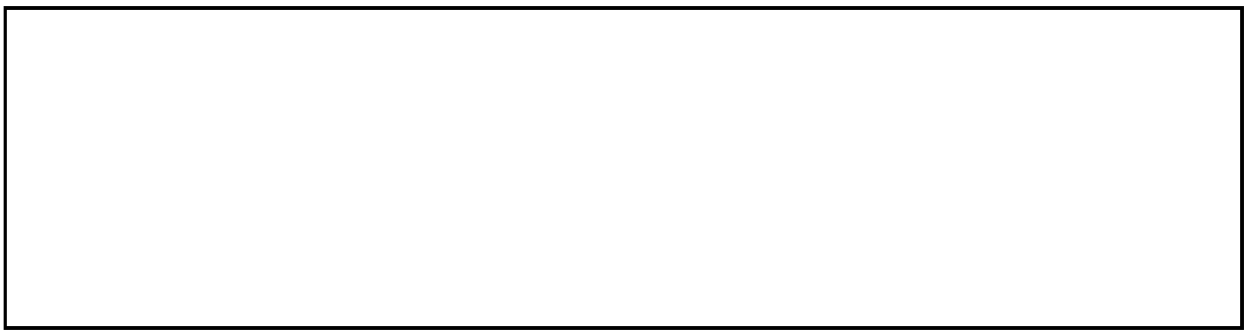


b1
b2
b6
b7A
b7C
b7E

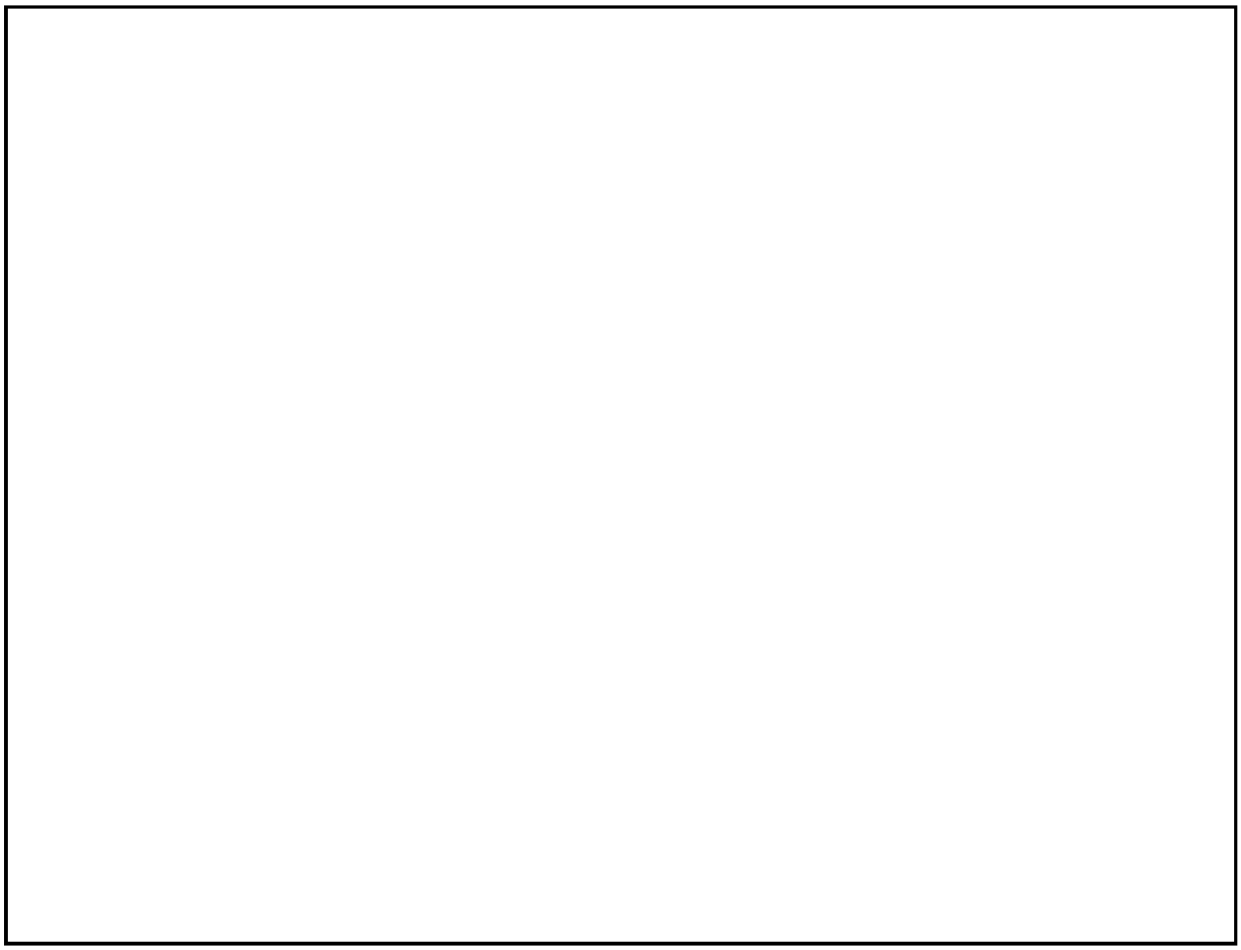
(S)

(S)

b5



b6
b7A
b7C



[redacted]

[redacted]

(S)

[redacted]

(S)

(S)

[redacted]

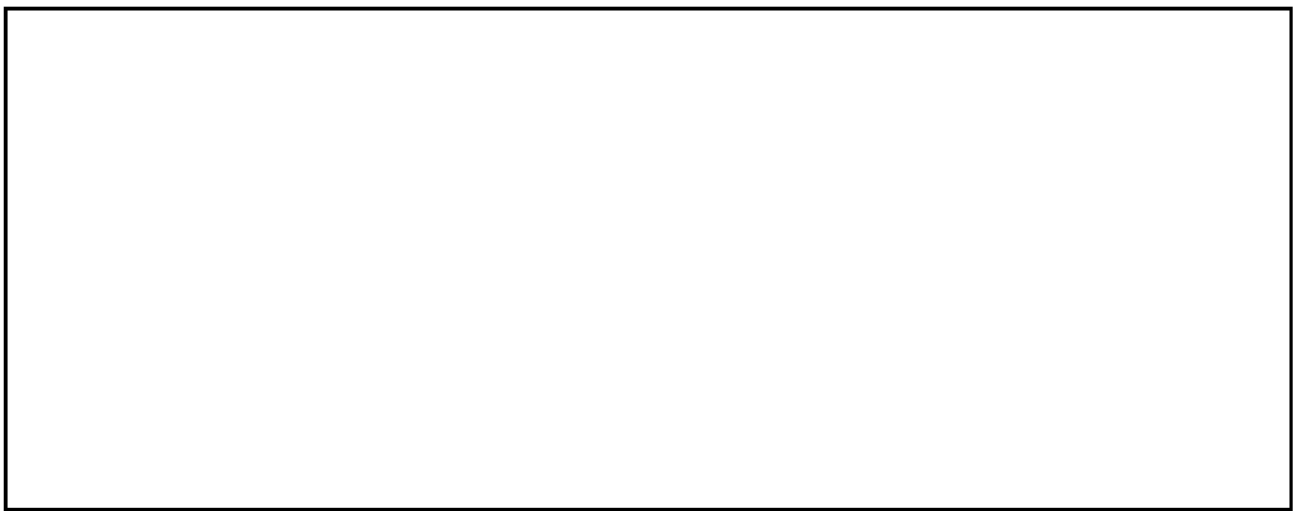
b1
b6
b7A
b7C

SECRET

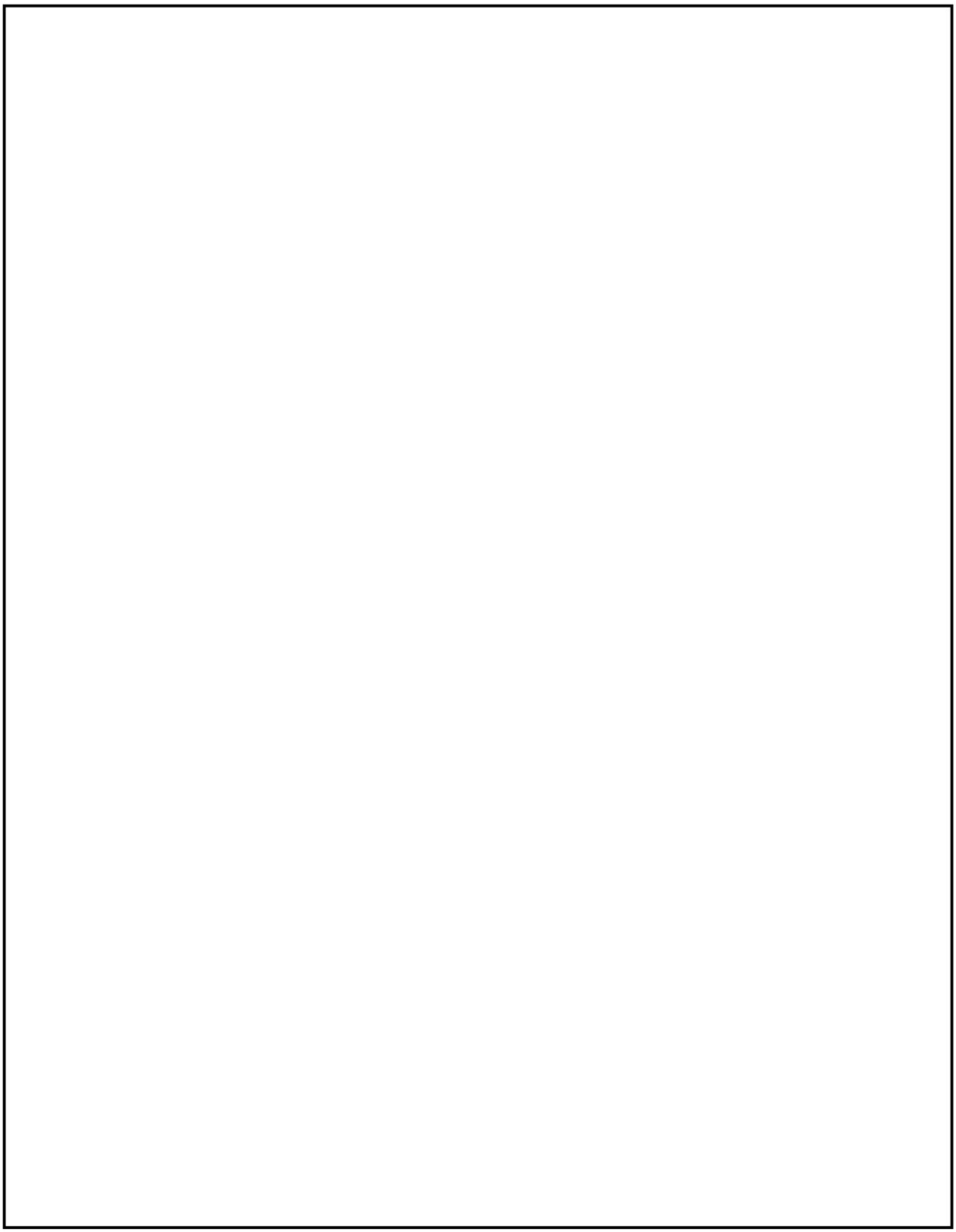
b5

~~SECRET~~

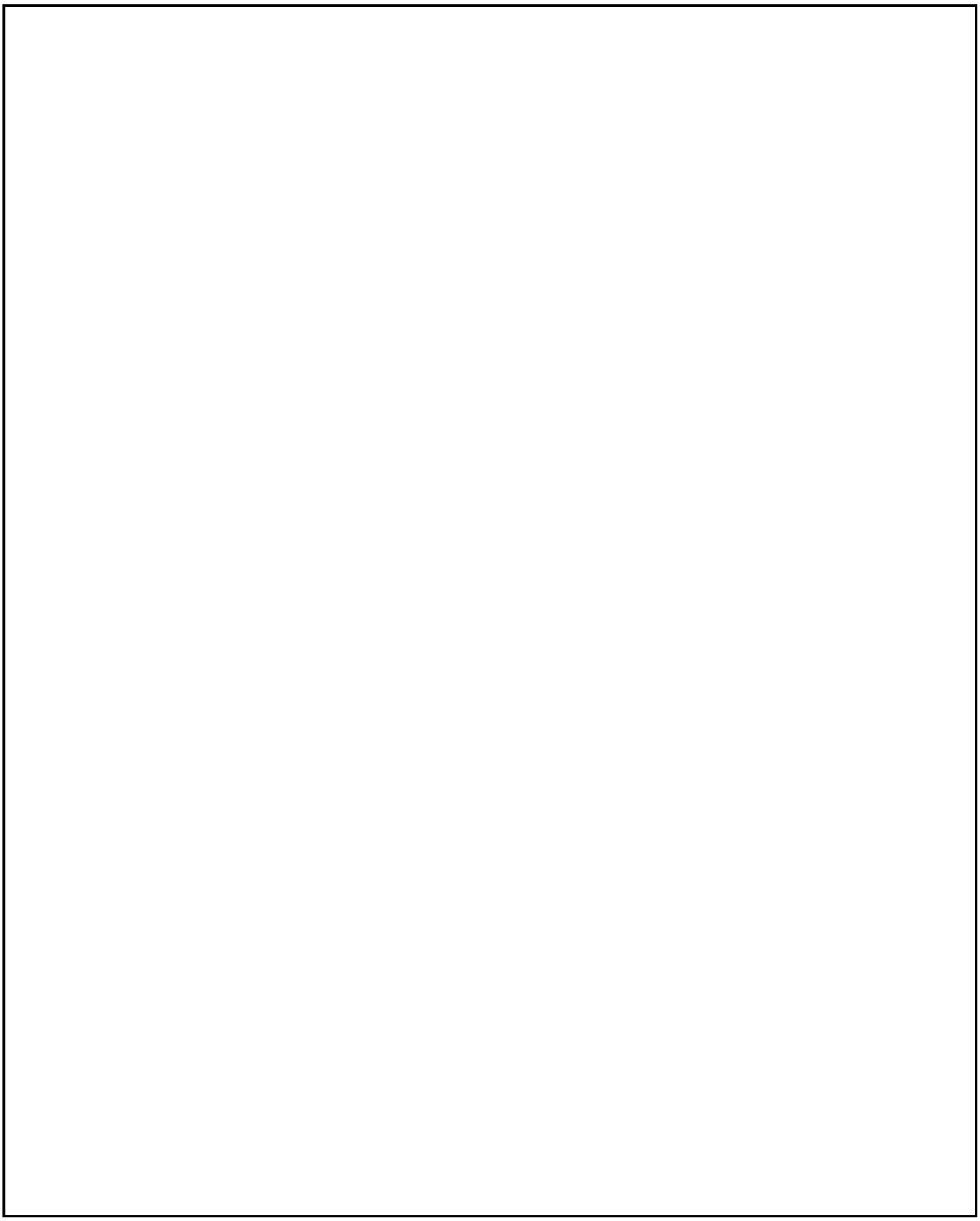
b5



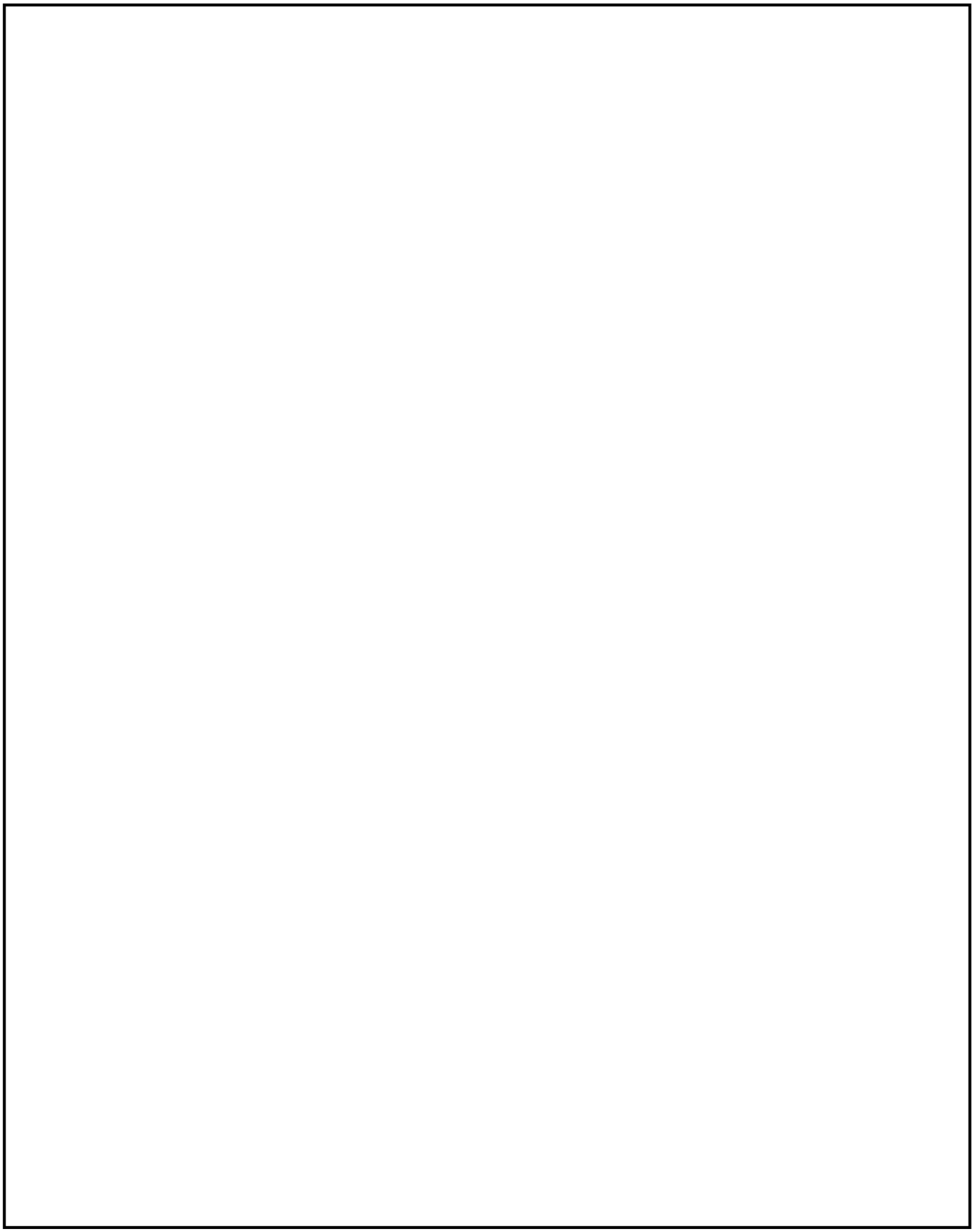
b6
b7A
b7C

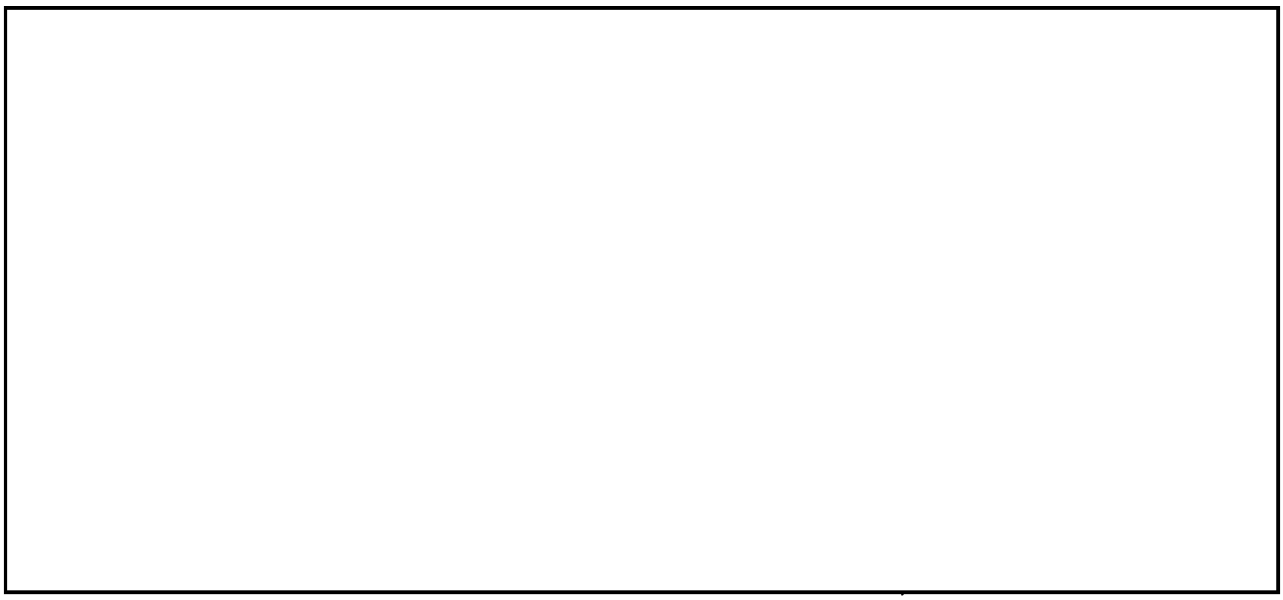


b2
b7A
b7E



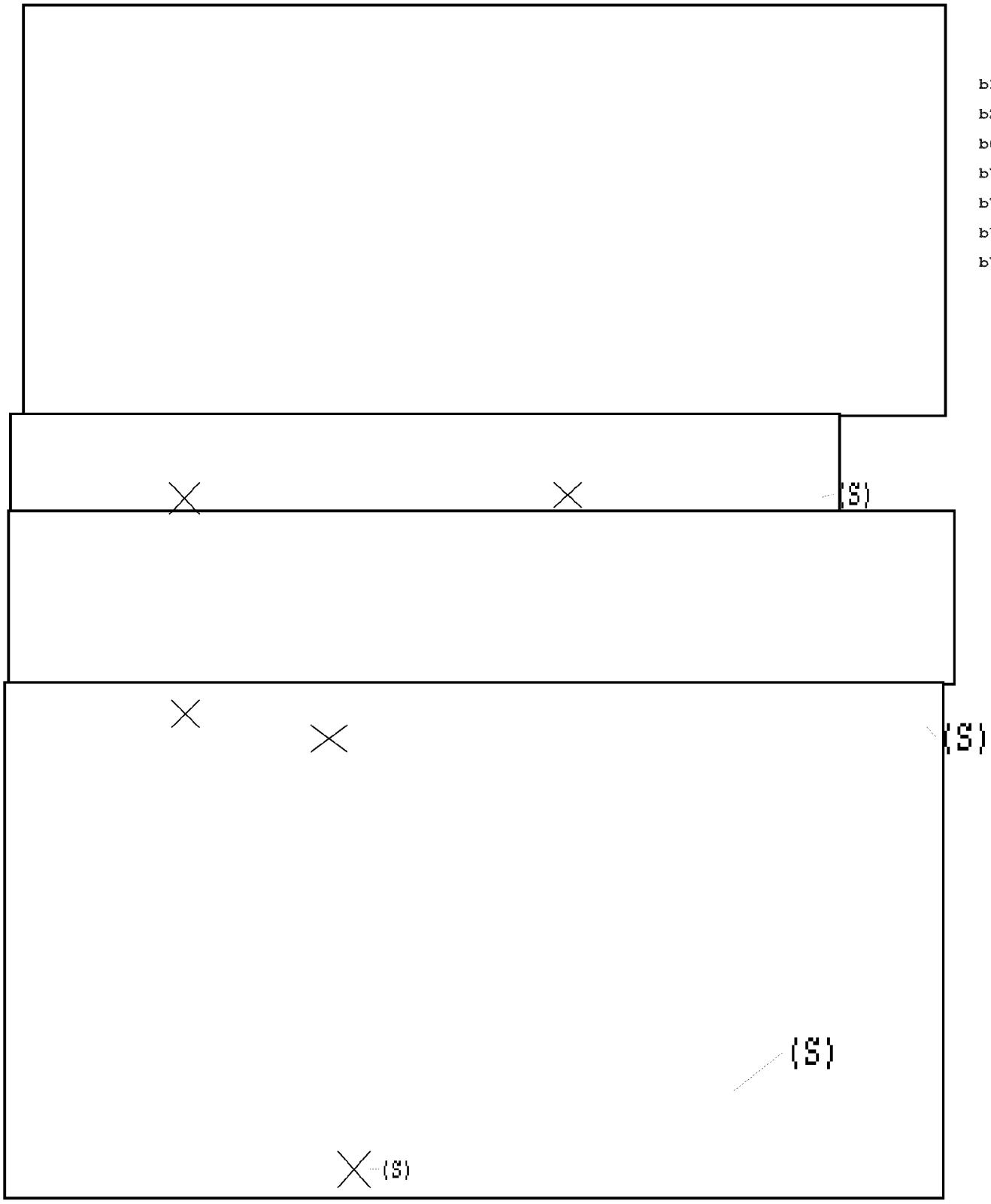
b2
b7A



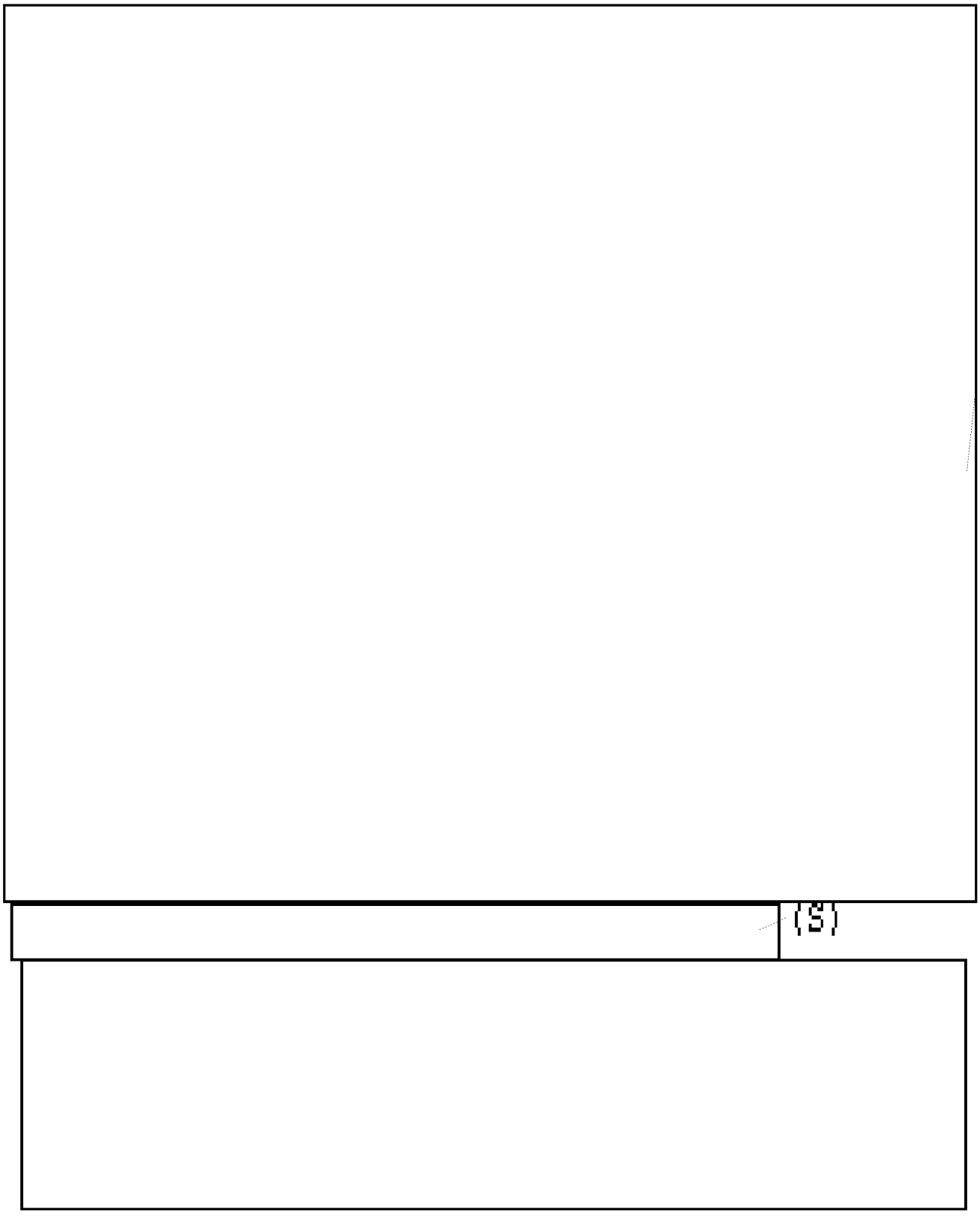


b2
b6
b7C
b7E

b1
b2
b6
b7A
b7C
b7D
b7E

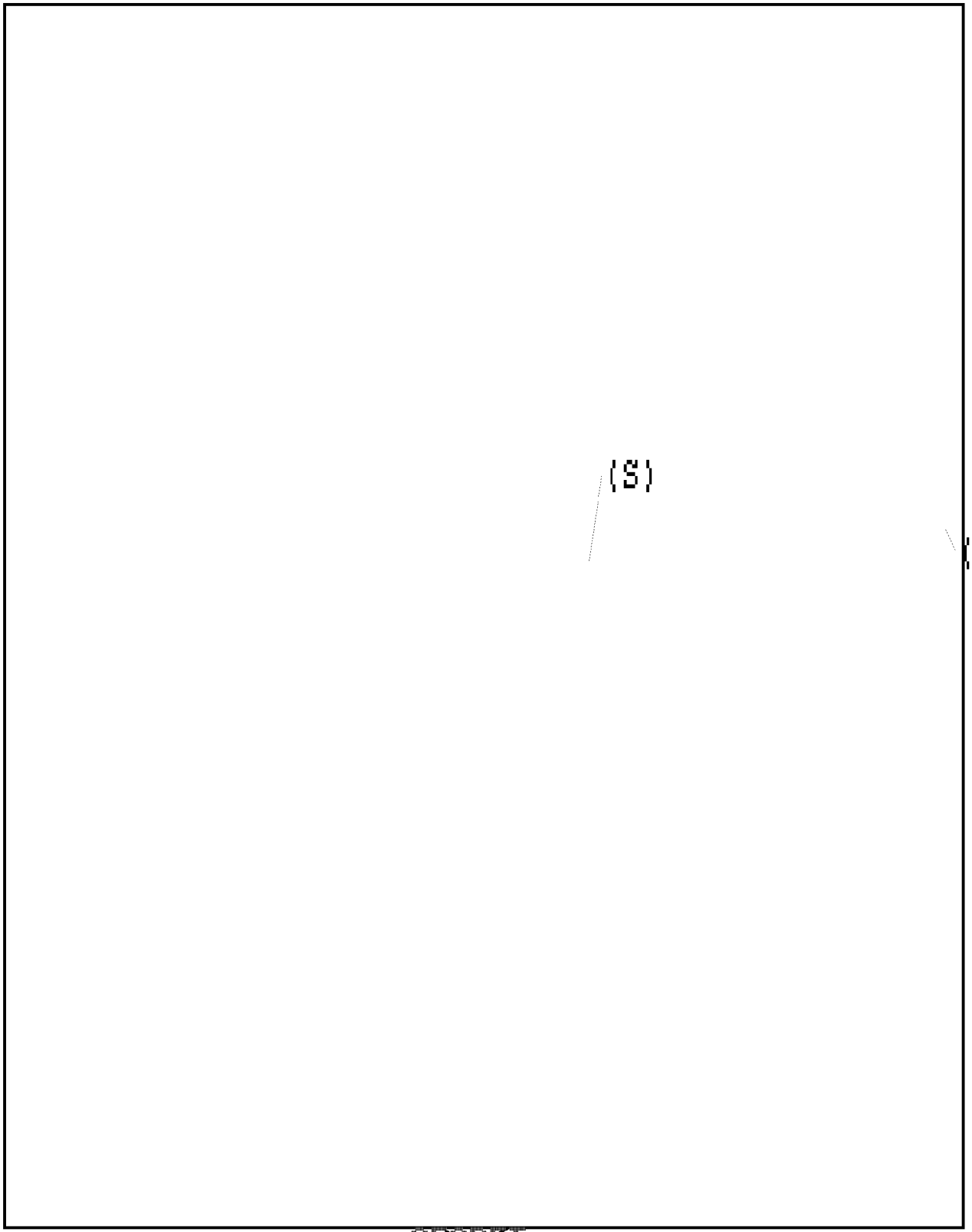


b1
b2
b6
b7A
b7C
b7D
b7E



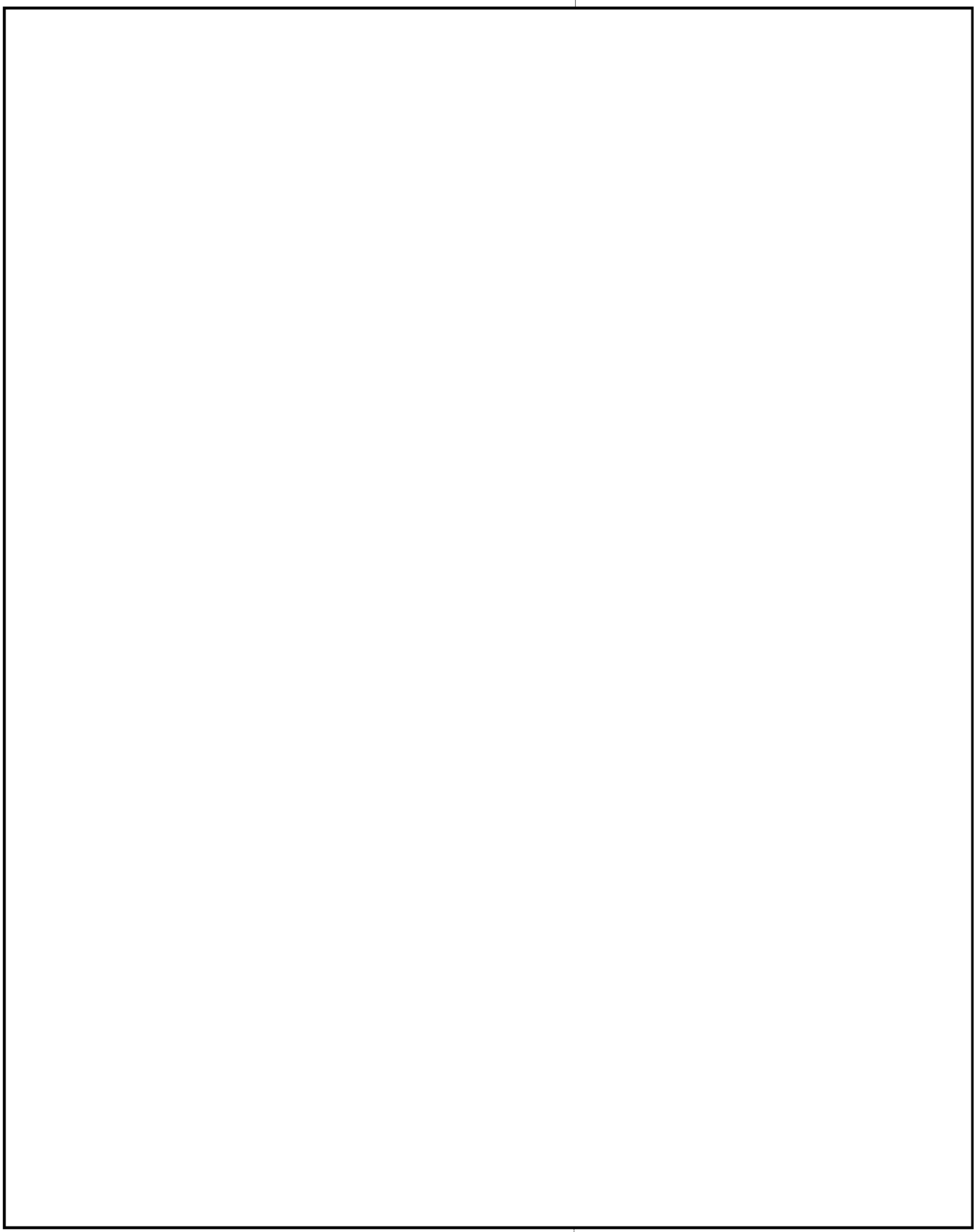
~~SECRET~~

b1
b2
b7A
b7E

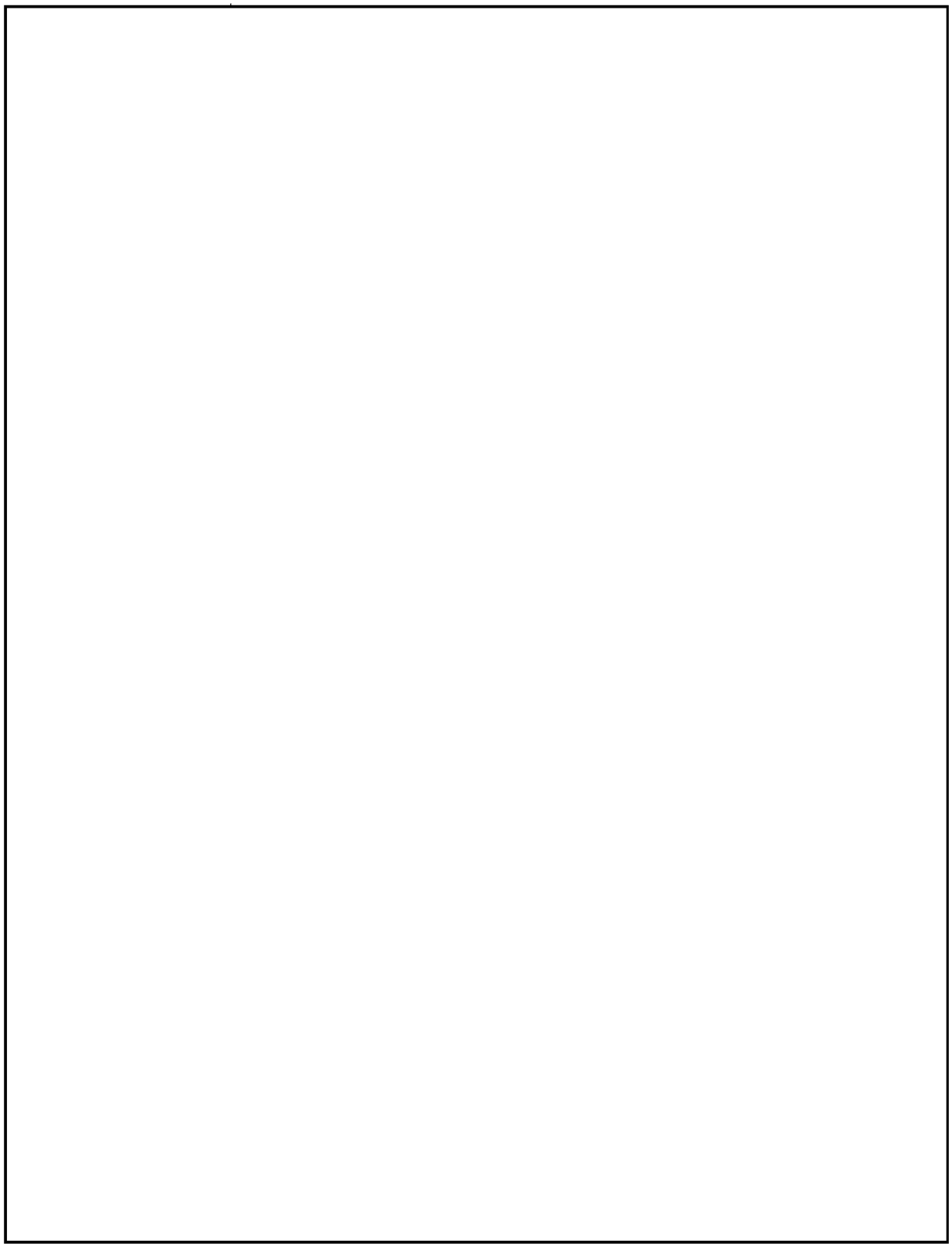


(S)

b1
b2
b7E

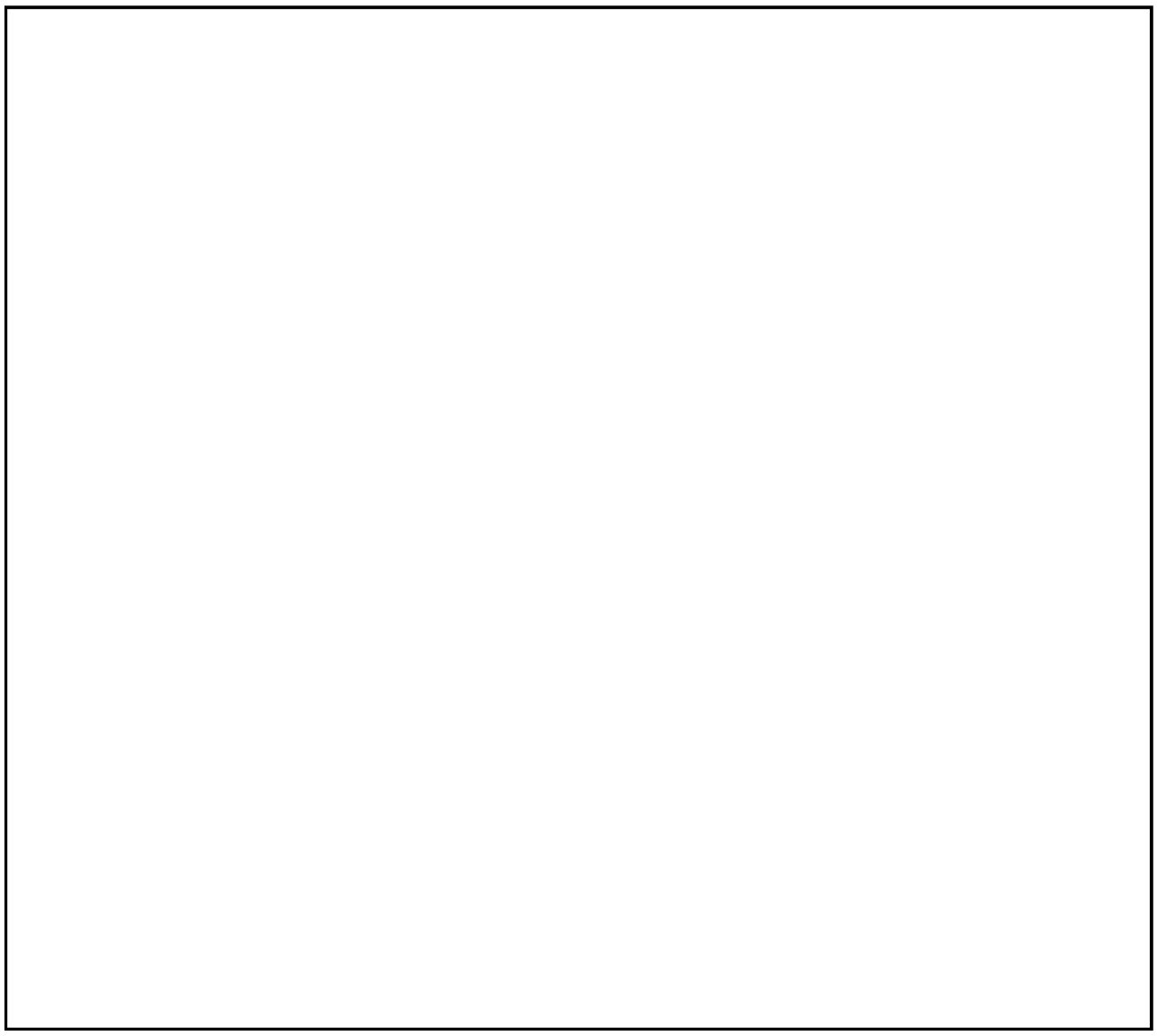


b2
b6
b7C
b7E



b2
b6
b7A
b7C
b7E

b2
b7E

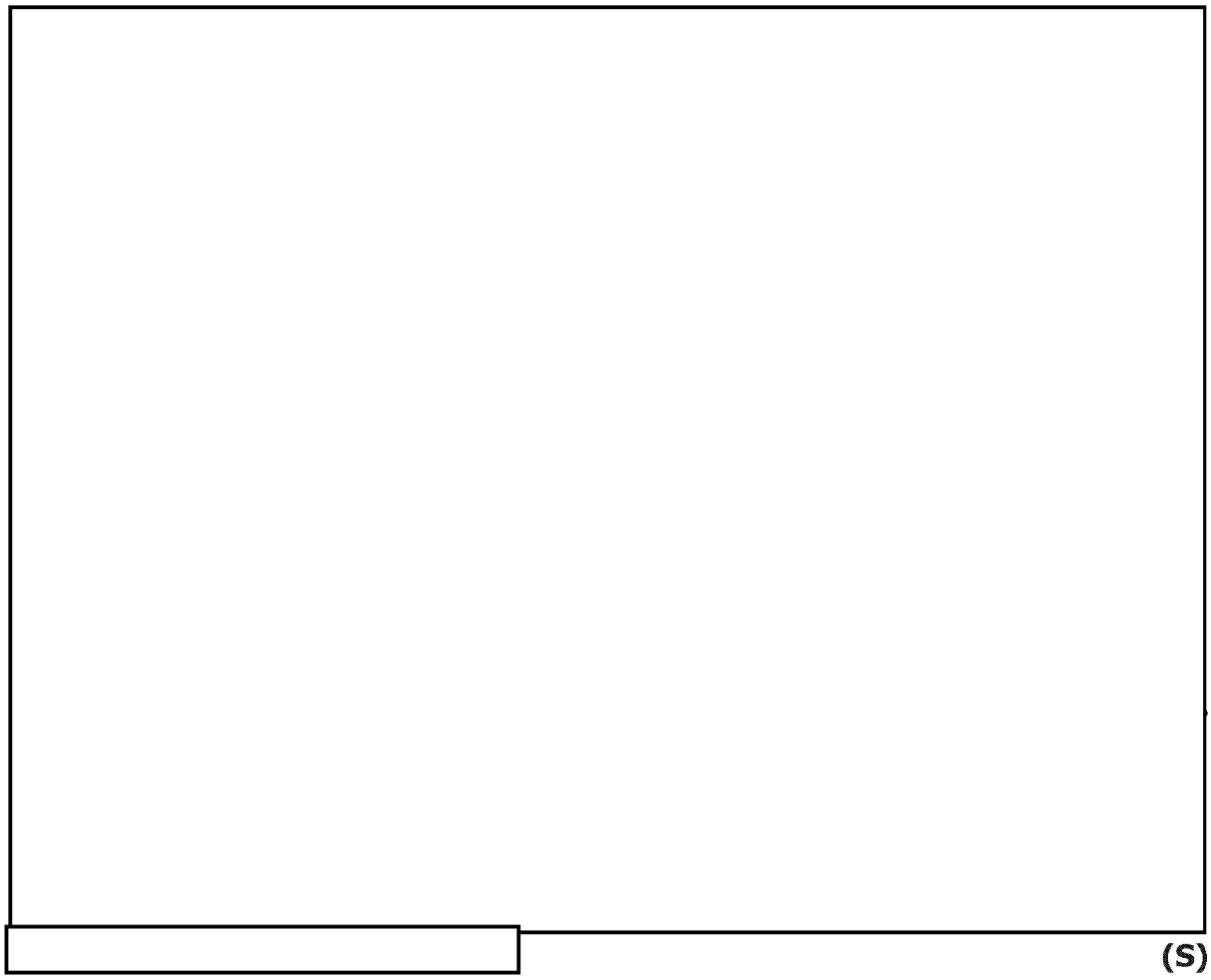


b1
b2
b7A
b7E

## Section 218 - Change in the "Primary Purpose" Standard of FISA

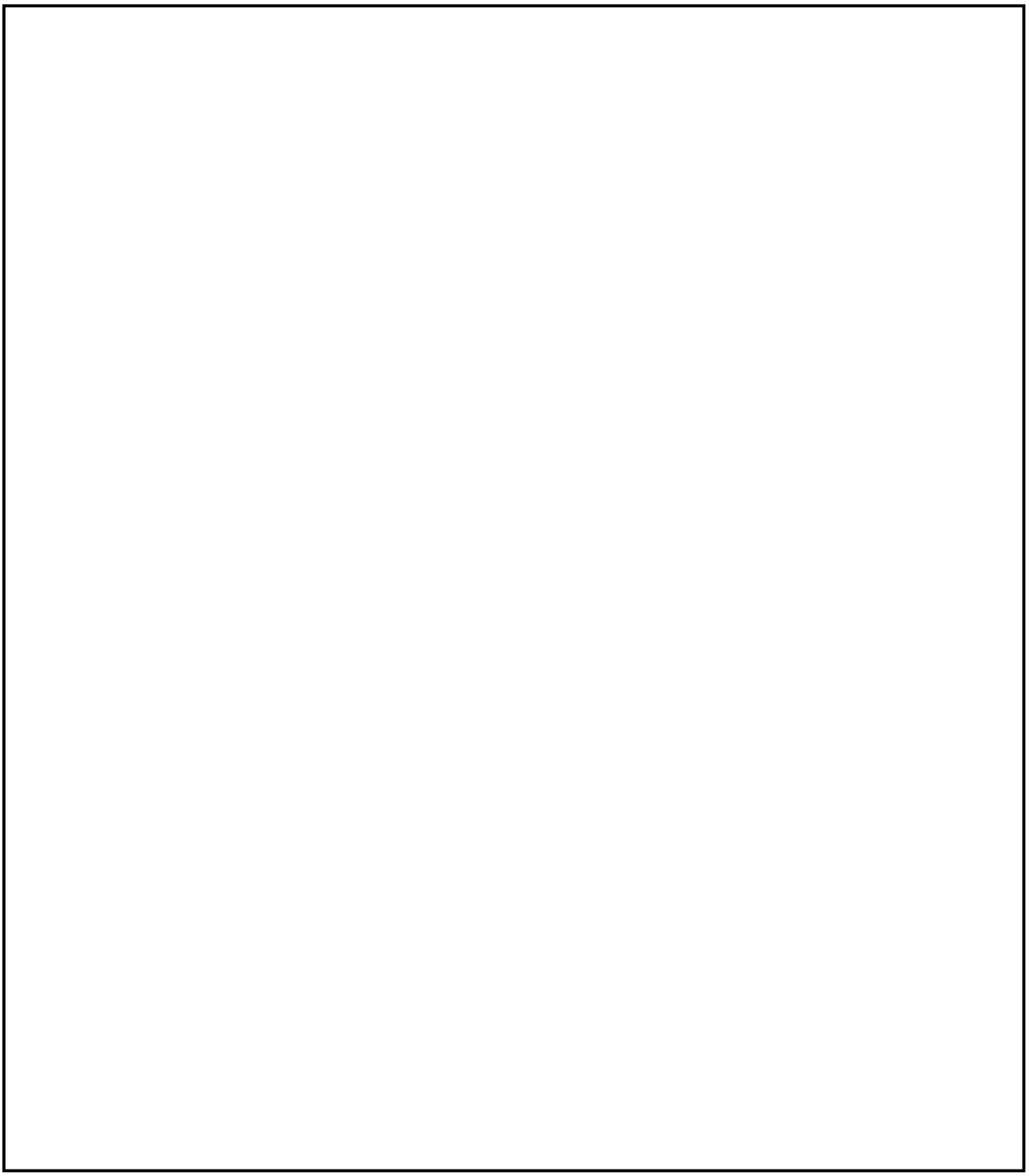
(S)

(S)



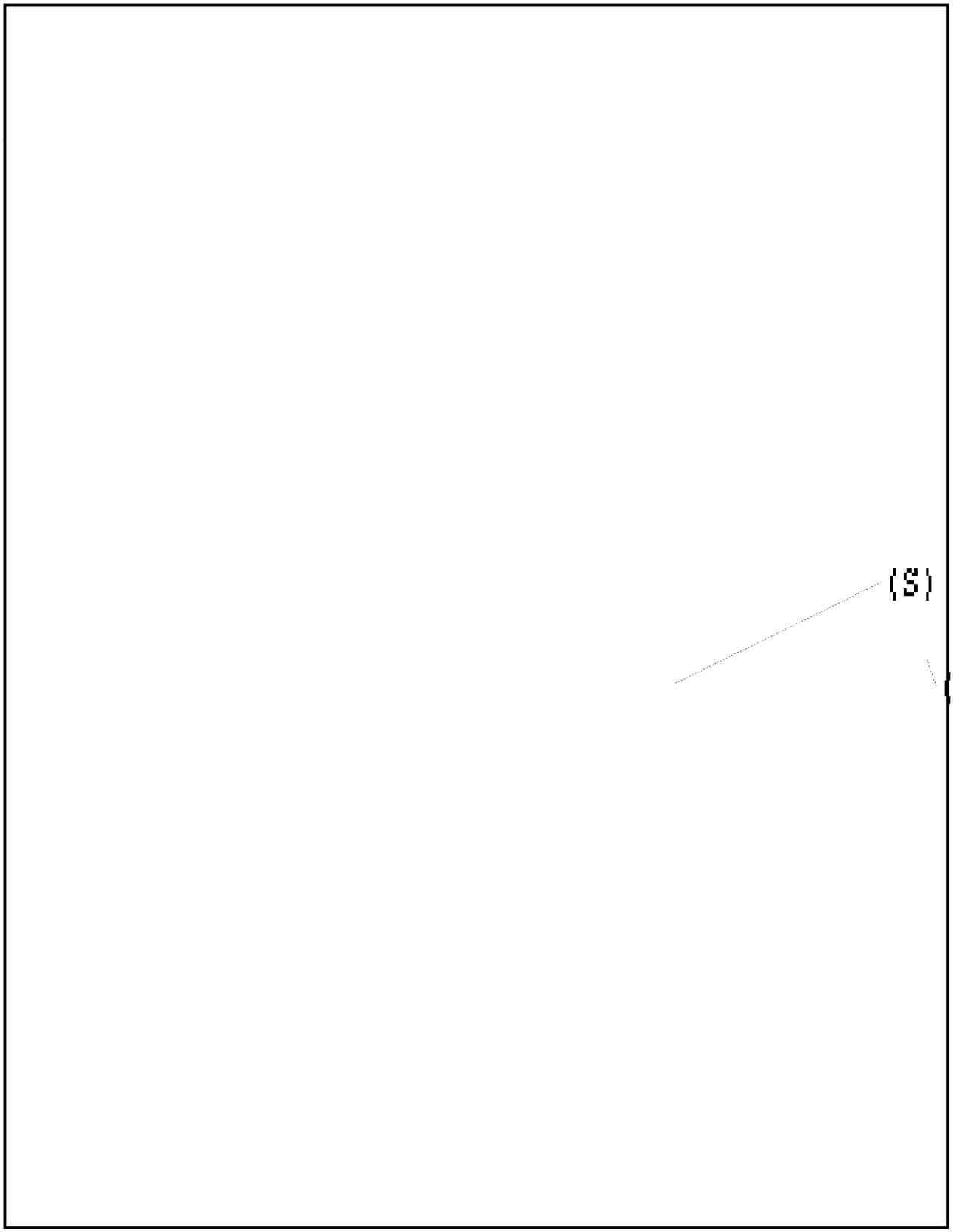
b1
b2
b6
b7A
b7E

(S)

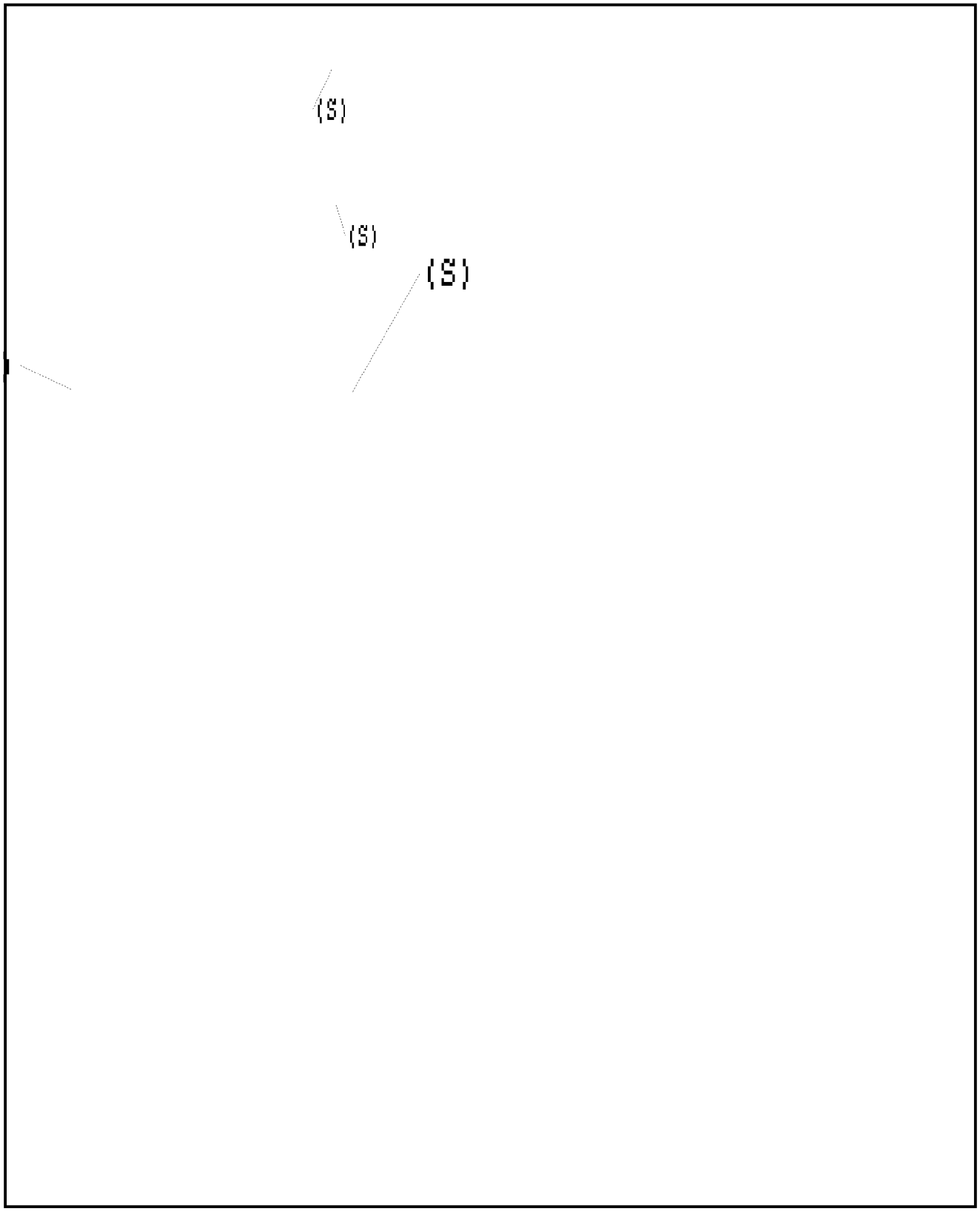


b2
b7E

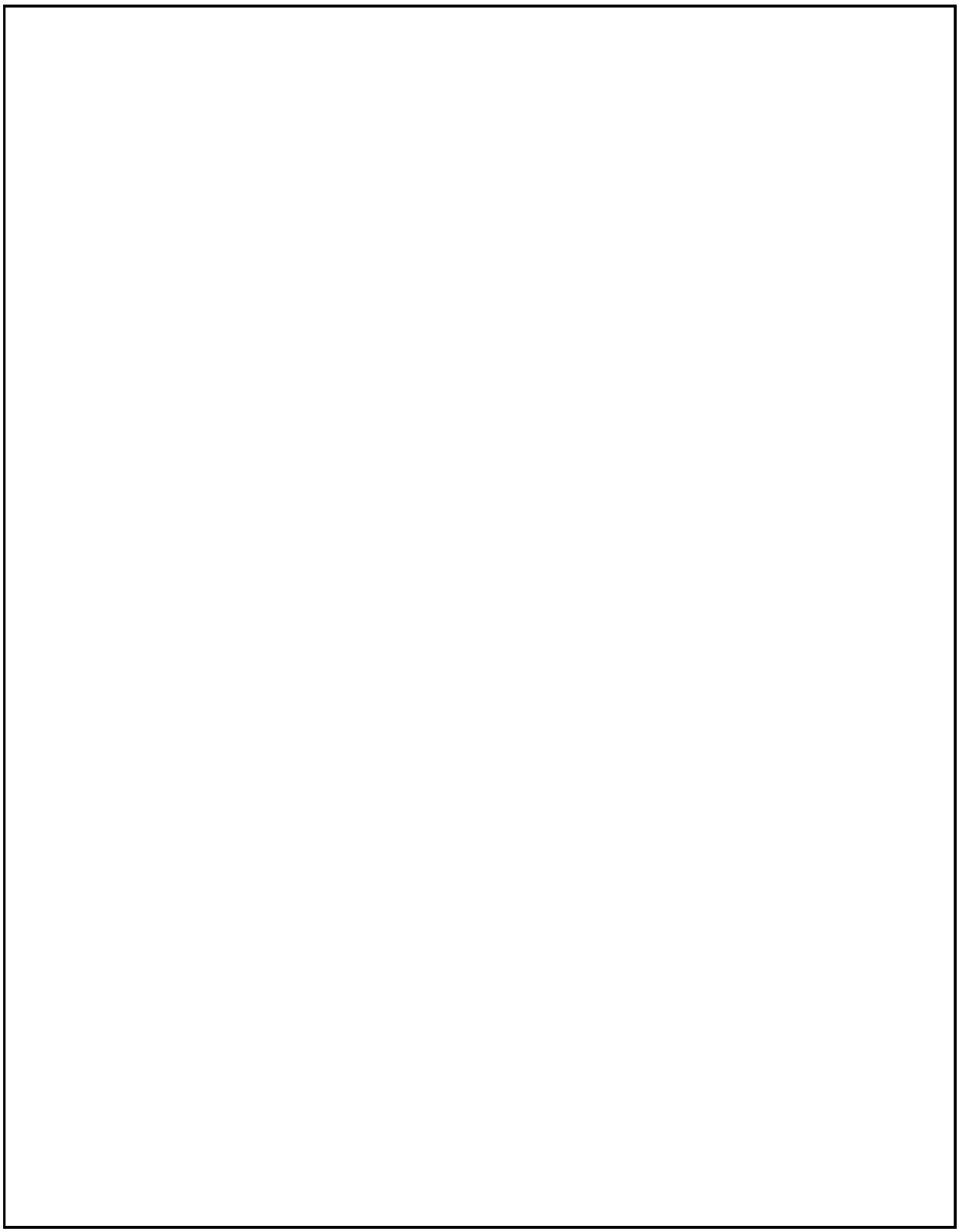
b1
b2
b6
b7A
b7C
b7E



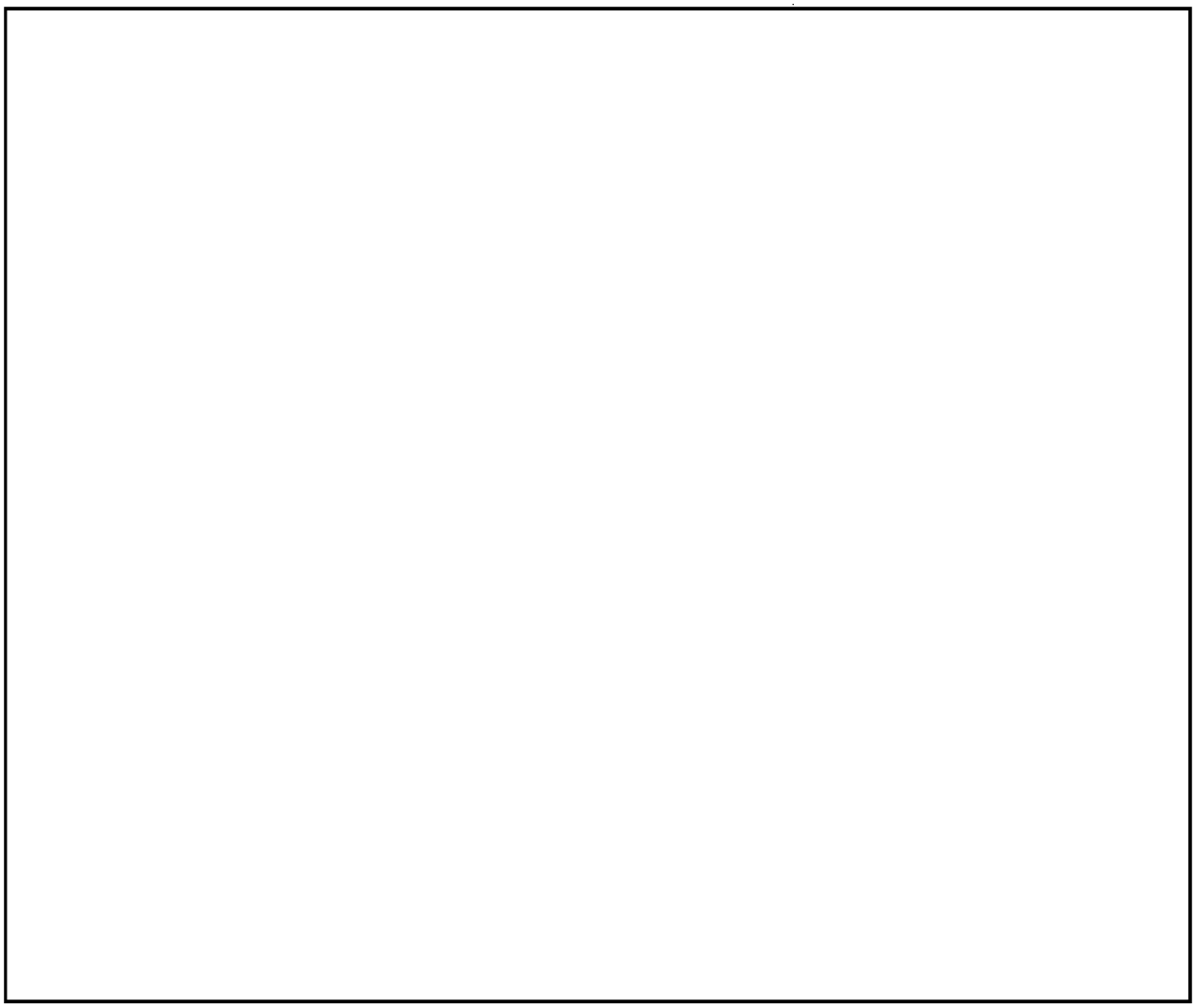
b1
b2
b6
b7A
b7C
b7E



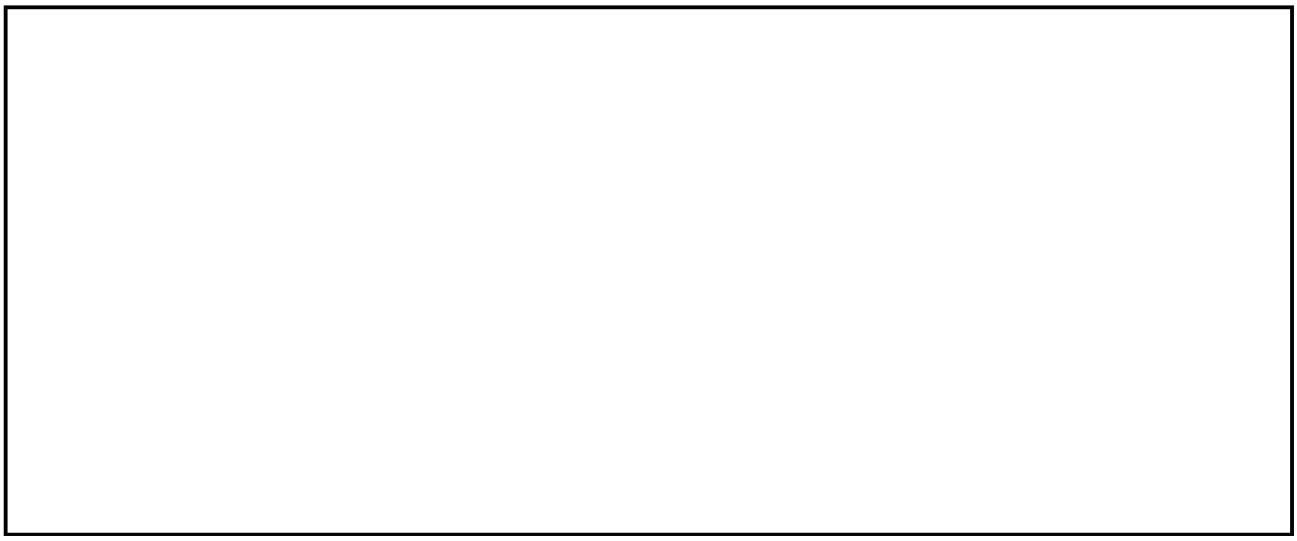
b2
b6
b7A
b7C
b7E



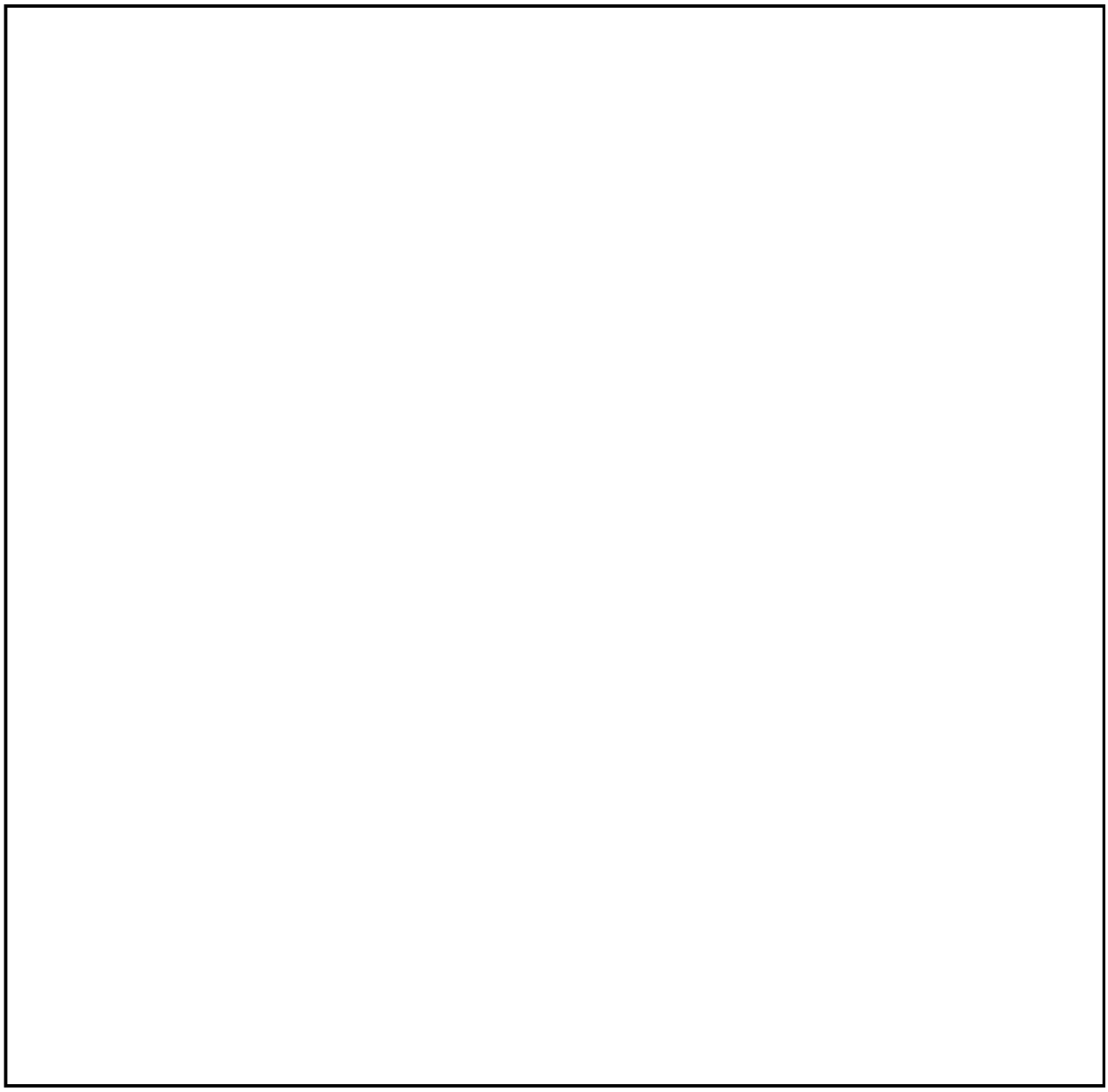
b2
b7E



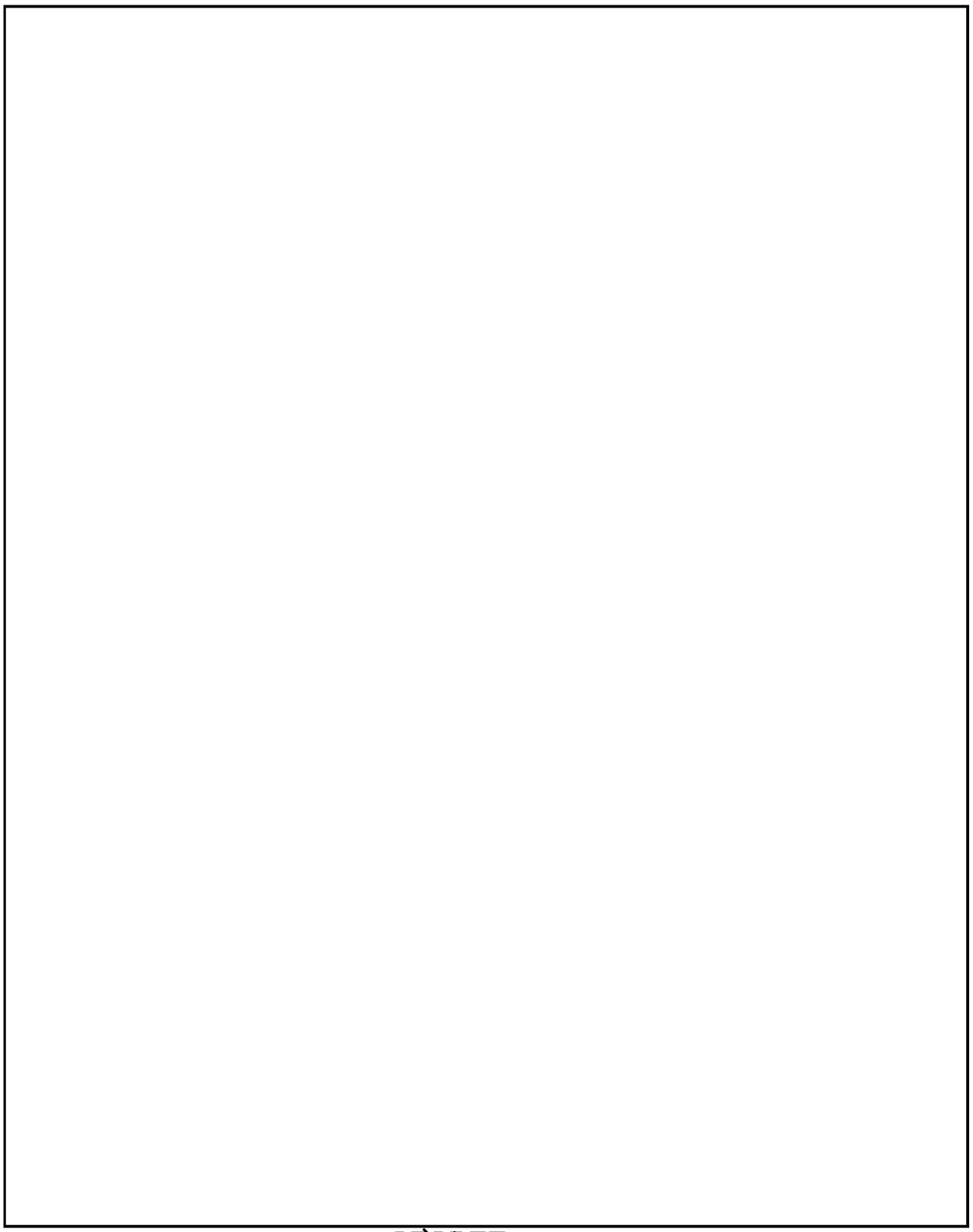
b5

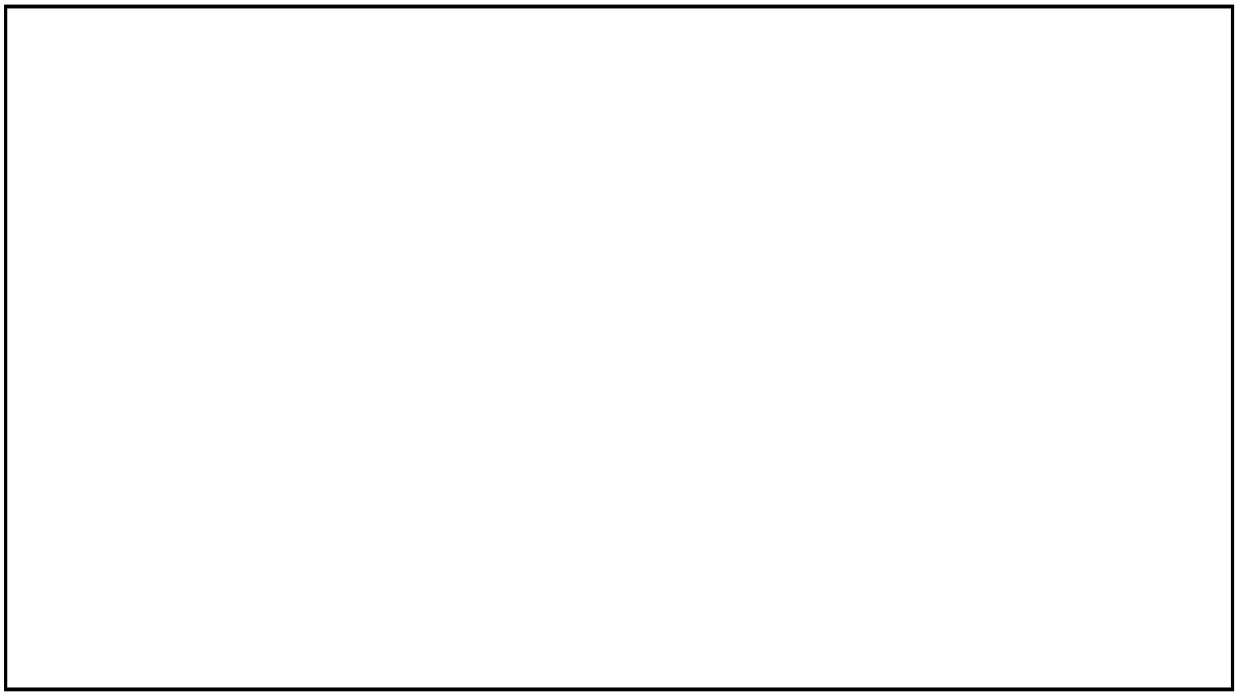


b2
b6
b7A
b7C
b7E



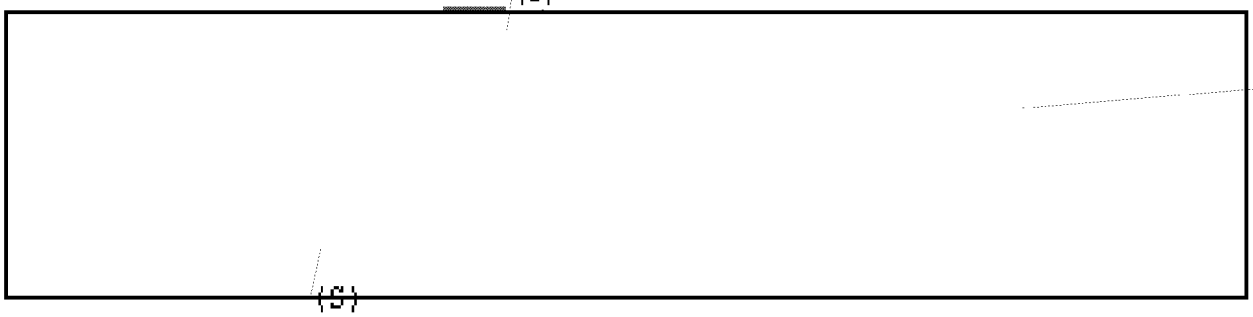
b2
b6
b7A
b7C
b7E





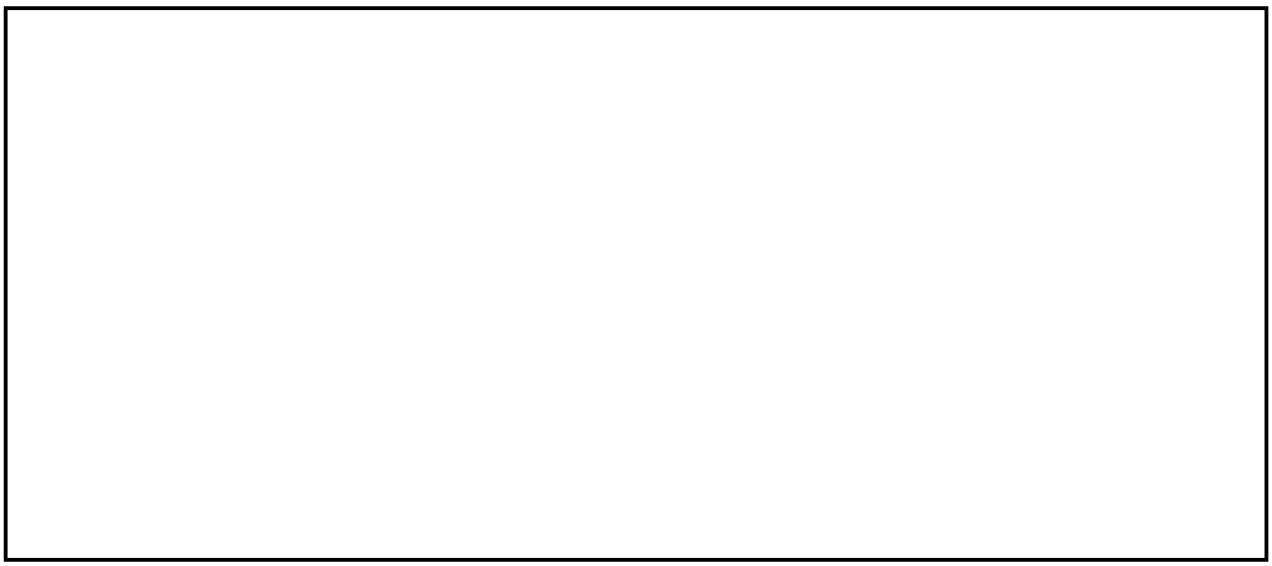
b1
b2
b6
b7A
b7C
b7E

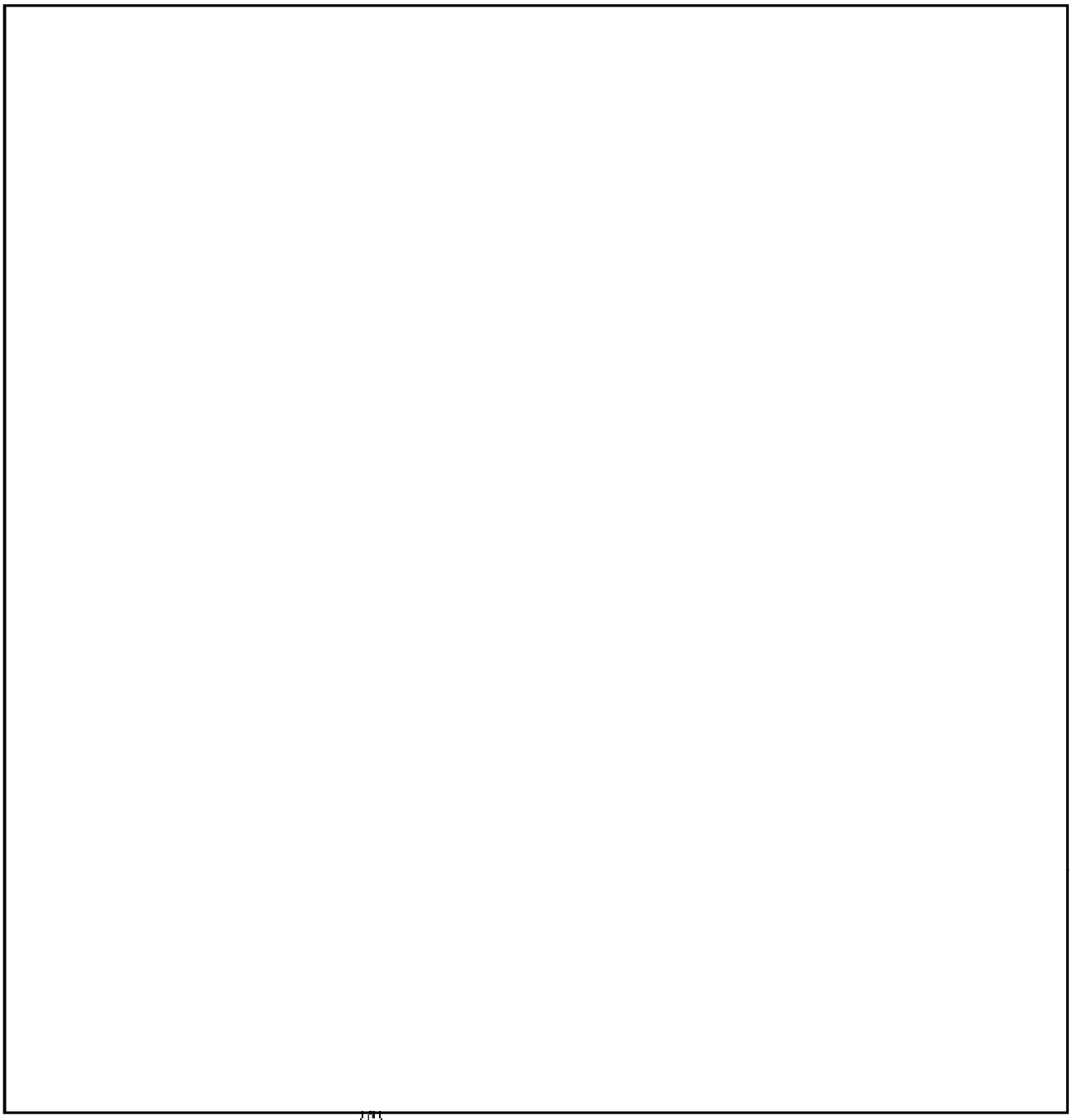
(S)



(S)

(S)

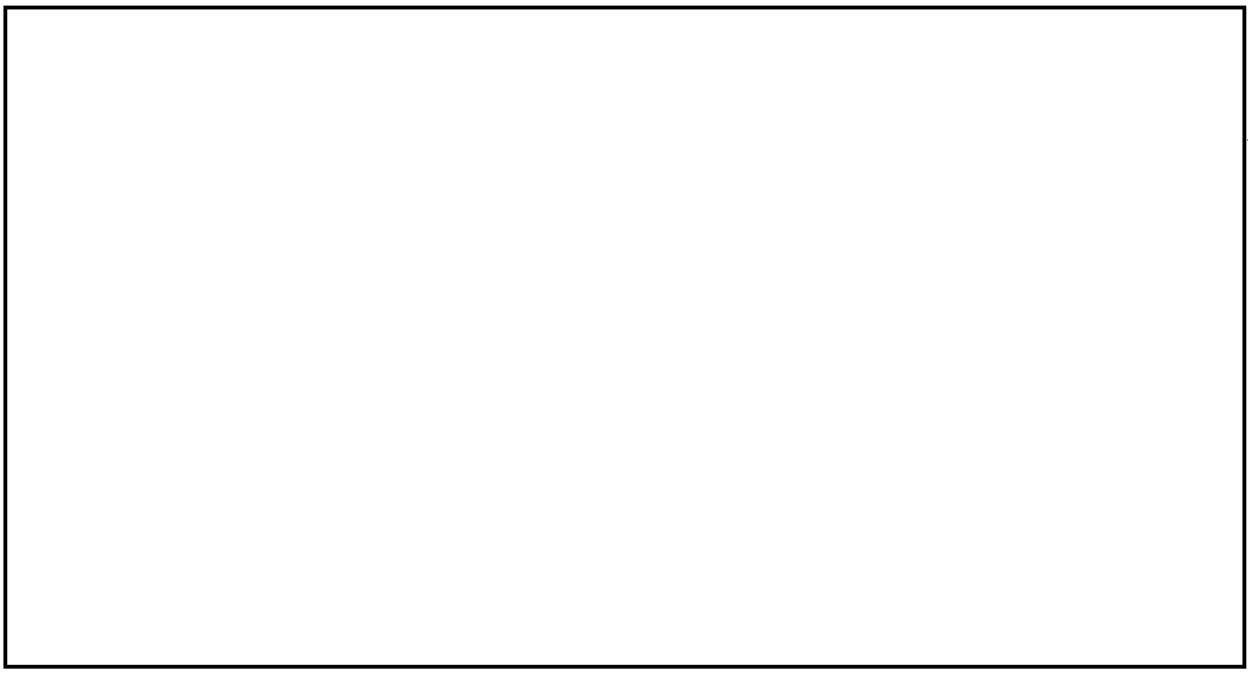




b1
b2
b6
b7A
b7C
b7D
b7E

(S)

b2
b7E



b2

## A. OPERATIONAL EXAMPLES OF USA PATRIOT ACT SUCCESSES (TEAM 1 [redacted] b7E

### 1. Sharing grand jury, Title III, and criminal investigative information (Sec. 203):

- FBINY obtained U.S. financial records through federal grand jury subpoenas. Information obtained from these records was also shared with the USIC and other terrorism cases were opened based on this intelligence.
- The Patriot Act enabled the FBI and Bureau of Prisons (BOP) to work together, sharing information regarding violations of Special Administrative Methods (SAM), in particular illegal communications between incarcerated terrorists and their attorneys (see Lynne Stewart conviction).

### 2. "Roving" FISA ELSUR authority:

### 3. Changes in FISA PR/TT authority (Sec. 214):

### 4. Changes in FISA business records authority:

b7A

### 5. Use of Library Records:

- [redacted]

## B. ADDITIONAL TOOLS & TWEAKS, i.e., WISH LIST

- One example of a need is an administrative subpoena power related to CTD efforts. We have that authority for Drugs and Health Care fraud matters, why not CT investigations which are just as important?

# Patriot Act Successes
## ITOS I/CONUS I

**Team 1**



- FB[ ]btained U.S. financial records through federal grand jury subpoenas. Information obtained from these records was also shared with the USIC and other terrorism cases were opened based on this intelligence. b2 b7E
- The Patriot Act enabled the FBI and Bureau of Prisons (BOP) to work together [ ] b2 b7E
- [ ] led to a recent indictment for making a false bomb threat to the government along with numerous 1001 violations. b2 b7E

**B. ADDITIONAL TOOLS**

- One example of a need is an administrative subpoena power related to CTD efforts. We have that authority for Drugs and Health Care fraud matters, why not CT investigations which are just as important?

**Team 2 & 3**

[ ]

- **Changes in FISA business records authority:** [ ] b2 b7E
- Section 215 of the Patriot Act allows the FBI to seek a FISA court order for any tangible materials such as books, records, papers, documents, and other items.

[ ]

**Section 214 Changes in FISA/PR/TT authority:**

- **Changes in FISA PR/TT authority:** [ ] b2 b7E

b2
b7E

- **Sharing grand jury, Title III, and criminal investigative information.**

**Team 4**

**Section 203 Sharing criminal investigative information:**

b2
b7E

- (U)

**Section 214 Changes in FISA/PR/TT authority:**

b2
b7E

- (U)

**Section 215 Changes in FISA business records authority:**

- (U)

b2
b7E

# CONUS 2 PATRIOT ACT EXAMPLES:

b6
b7C
b7A

1. Subje

Predication:

(S)

(S)

b1
b2
b7E
b6
b7C
b7A

Patriot Act usage:

(S)

b1
b2
b7E
b7A

(S)

b1
b6
b7C
b7A

**From:** [redacted] (OGC) (FBI)
**Sent:** Wednesday, March 23, 2005 11:49 AM
**To:** [redacted] (CTD) (FBI)
**Cc:** [redacted] (OCA) (FBI)
**Subject:** FW: Responses for Director's Testimony/Patriot Act

b6
b7C

**UNCLASSIFIED**
**RECORD 315N-SE**

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-23-2005 BY 65179 DMH/JHF 05-CV-0845

#3
-----Original Message-----
**From:** [redacted] (OGC)(FBI)
**Sent:** Tuesday, March 22, 2005 5:10 PM
**To:** [redacted] OGC) (FBI)
**Subject:** FW: Responses for Director's Testimony/Patriot Act

b6
b7C

**UNCLASSIFIED**
**RECORD 315N-SE**

-----Original Message-----
**From:** [redacted] (CTD) (FBI)
**Sent:** Friday, March 18, 2005 7:20 PM
**To:** [redacted] CTD) (FBI)
**Cc:** [redacted] OGC)(FBI)
**Subject:** FW: Responses for Director's Testimony/Patriot Act

b6
b7C

**UNCLASSIFIED**
**RECORD 315N-SE**

Patriot Act info

[redacted]
CTD/ITOS 1/Conus IV
[redacted]

b6
b7C

b6
b7C

-----Original Message-----
**From:** [redacted] CTD) (FBI)
**Sent:** Friday, March 18, 2005 11:15 AM
**To:** [redacted] (CTD) (FBI)
**Cc:** [redacted] (CTD) (FBI)
**Subject:** Responses for Director's Testimony/Patriot Act

b6
b7C

**UNCLASSIFIED**
**RECORD 315N-SE**

b6
b7C

[redacted]

[redacted] sked that we provide examples of Patriot Act info/examples from our division's of responsibility, which are being compiled for the director's testimony. This is a [redacted] example of timely criminal investigative/intel info

b2
b7E

b2
b7E

sharing with the Department of Defense (Army):

(U)

Thanks for passing this along.

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

**From:** (OGC) (FBI)
**Sent:** Wednesday, March 23, 2005 11:49 AM
**To:** (CTD) (FBI)
**Cc:** (OCA) (FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

b6
b7C

DATE: 09-23-2005
CLASSIFIED BY 65179 DMH/JHF
REASON: 1.4 (C ,D)
DECLASSIFY ON: 09-23-2030

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

#2
-----Original Message-----
**From:** (OGC)(FBI)
**Sent:** Tuesday, March 22, 2005 5:09 PM
**To:** (OGC) (FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

-----Original Message-----
**From:** CTD) (FBI)
**Sent:** Monday, March 21, 2005 12:53 PM
**To:** CTD) (FBI)
**Cc:** (OGC)(FBI)
**Subject:** RE: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Thanks. is handling that, I'm not doing anything about the Patriot Act tasking.

b6
b7C

CTD/ITOS-1

b6
b7C

-----Original Message-----
**From:** (CTD) (FBI)
**Sent:** Friday, March 18, 2005 7:18 PM
**To:** (CTD) (FBI)
**Cc:** (OGC)(FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Patriot Act tasking

b6
b7C

SECRET

CTD/ITOS 1/Conus IV

[redacted]

b6
b7C

-----Original Message-----
**From:** [redacted] (CTD) (FBI)
**Sent:** Friday, March 18, 2005 11:01 AM
**To:** [redacted] (CTD) (FBI)
**Cc:** [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
**Subject:** Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

b1

[redacted]

Here is a bullet for the [redacted] division:

b2
b6
b7C
b7E

(S) [redacted]

(S)

Thanks,

[redacted]

IA [redacted]
CTD/ITOS I/CONUS IV

[redacted]

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SECRET~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

SECRET

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

**From** [redacted] (OGC) (FBI)
**Sent:** Wednesday, March 23, 2005 11:49 AM
**To** [redacted] TD) (FBI)
**Cc** [redacted] (OCA) (FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

DATE: 09-23-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C , D)
DECLASSIFY ON: 09-23-2030

#4
-----Original Message-----
**From:** [redacted] (OGC)(FBI)
**Sent:** Tuesday, March 22, 2005 5:11 PM
**To** [redacted] (OGC) (FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

b6
b7C

-----Original Message-----
**From:** [redacted] CTD) (FBI)
**Sent:** Friday, March 18, 2005 7:18 PM
**To:** [redacted] TD) (FBI)
**Cc:** [redacted] OGC)(FBI)
**Subject:** FW: Bullets for Director's Senate Testimony

b6
b7C

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

Patriot Act tasking

[redacted]
CTD/ITOS 1/Conus IV
[redacted]
-----Original Message-----
**From:** [redacted] (CTD) (FBI)
**Sent:** Friday, March 18, 2005 11:01 AM
**To** [redacted] (CTD) (FBI)
**Cc:** [redacted] (CTD) (FBI); [redacted] (CTD) (FBI); [redacted] (CTD) (FBI)
**Subject:** Bullets for Director's Senate Testimony

SECRET

~~SENSITIVE BUT UNCLASSIFIED~~
~~NON-RECORD~~

b2
b7C

[redacted]
~~There is a bullet for the~~ [redacted] division:

b6
b7C

(U) [redacted]

b2 , b7E

[redacted] (S)

b1
b6
b7C
b2
b7E

Thanks,

[redacted]

IA [redacted]
CTD/ITOS I/CONUS IV

b6
b7C

[redacted]

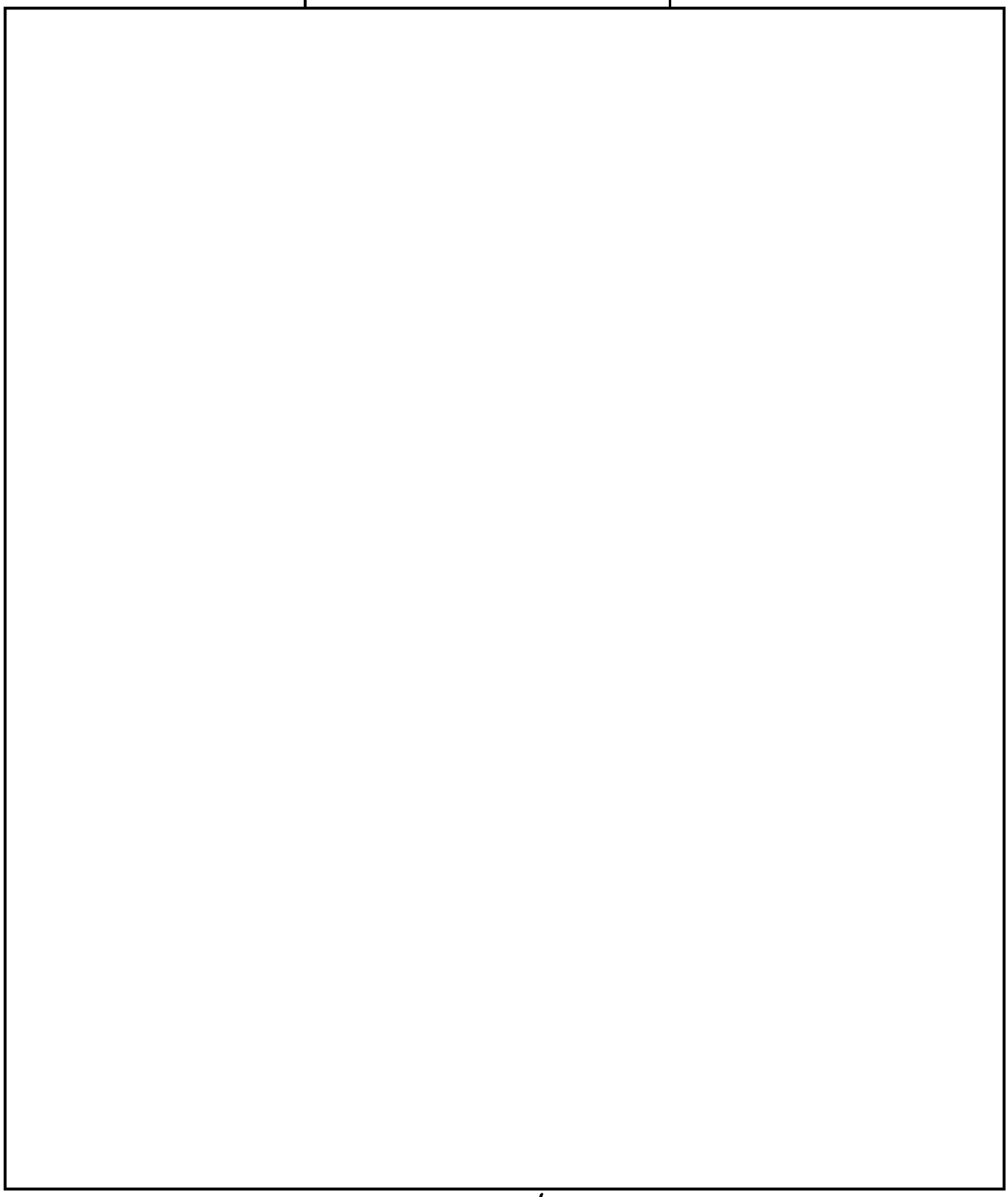
~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

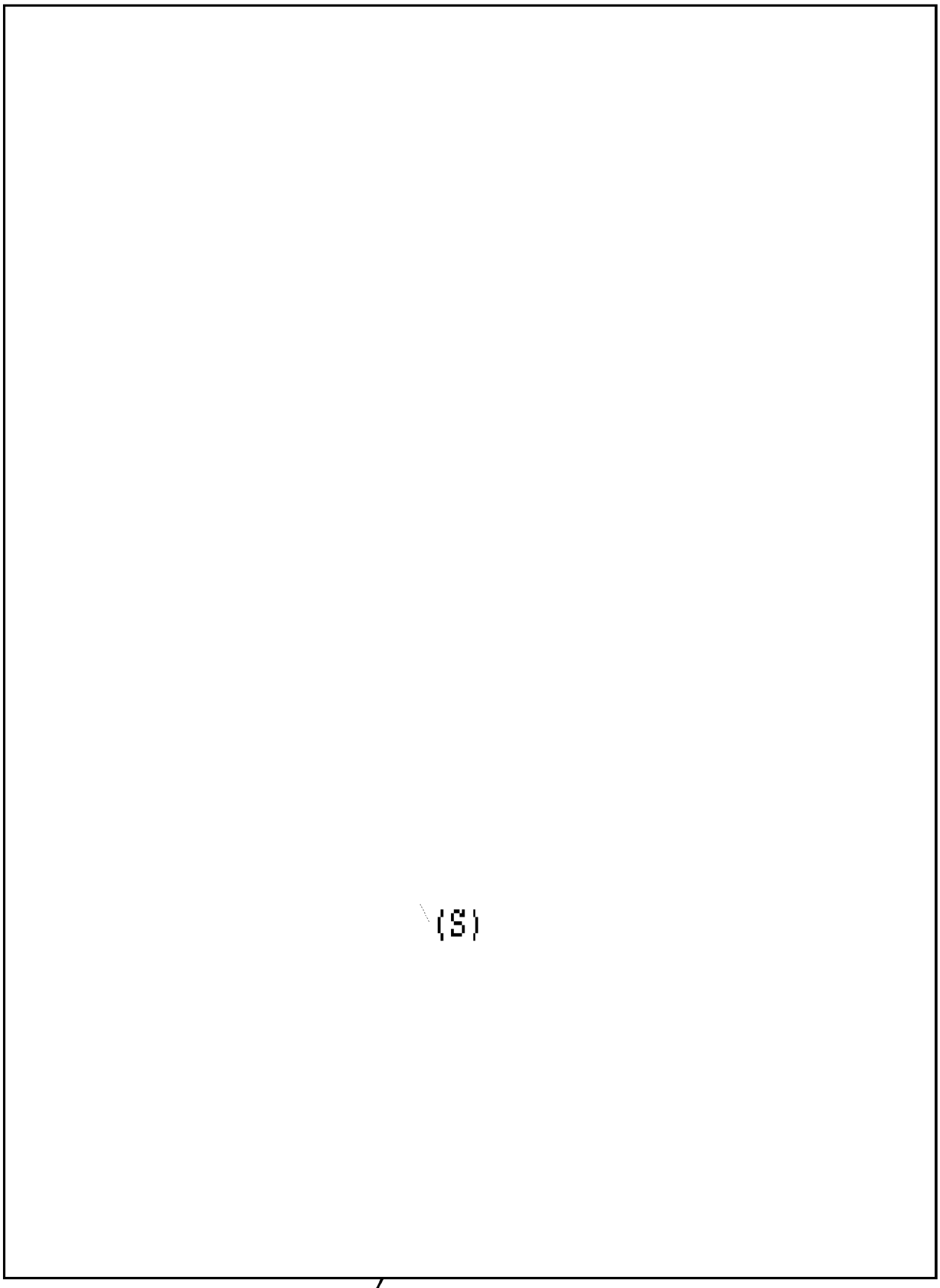
~~SENSITIVE BUT UNCLASSIFIED~~

~~SENSITIVE BUT UNCLASSIFIED~~

SECRET

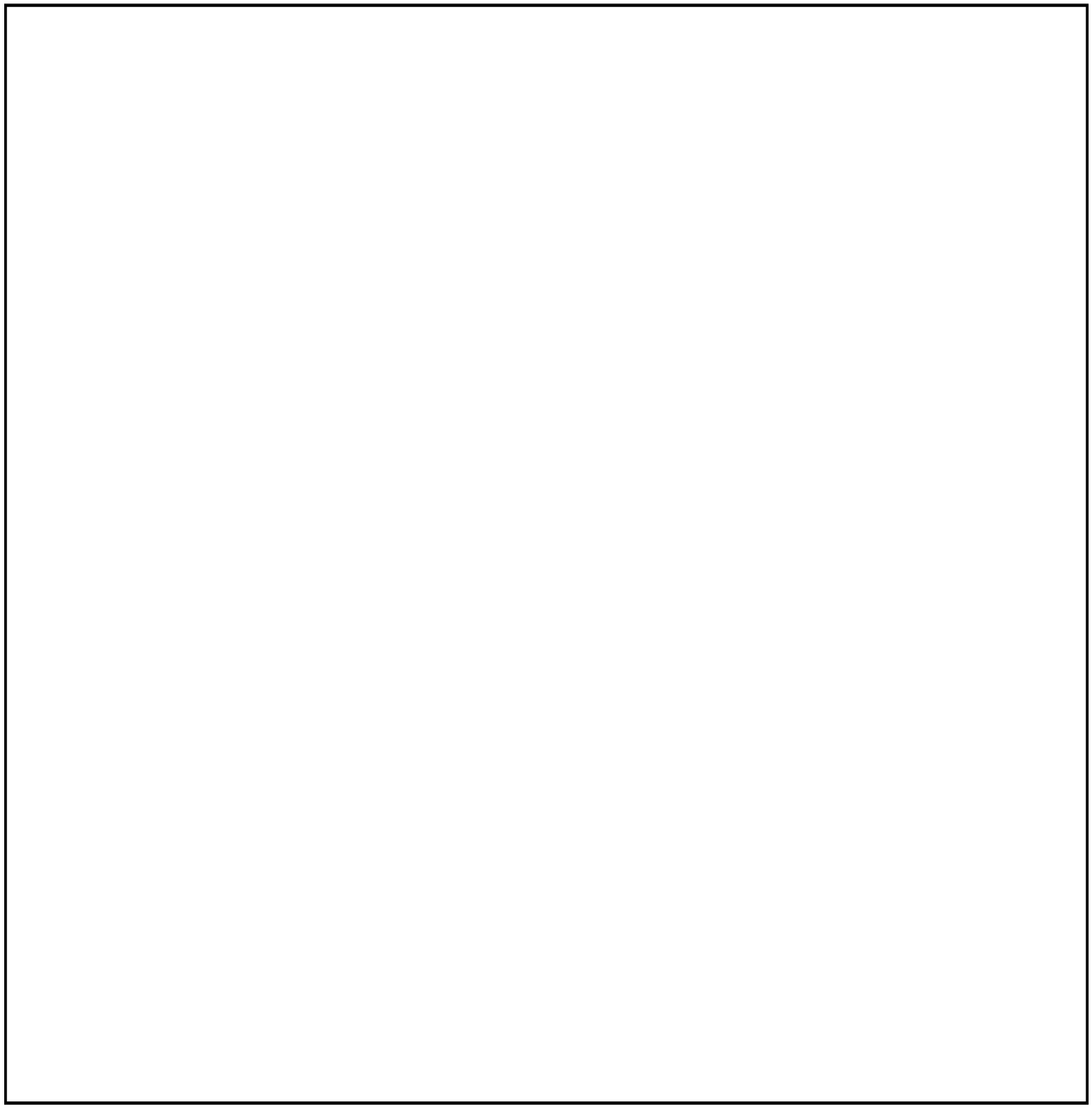


b1
b2
b7E



(S)

b2
b5
b7E



**PATRIOT Act Response**
**WMD/Domestic Terrorism Operations Section (WMD/DTOS)**
**FBIHQ**
**03/23/2005**

**Item #1**
**Special Events Management Unit/Civil Aviation Security Program (SEMU/CASP)**
**FBIHQ POC: SSA** [redacted] b6 b7C

The Patriot Act was used by the [redacted] Field Office to charge David Banach with one (1) count of Title 18 Section 1993 (a) 5 (Terrorist attacks and other acts of violence against mass transportation systems with reckless disregard for the safety of human life) On or about January 5, 2005. Mr. Banach was the individual who "lazed" a charter aircraft coming into Teteboro Airport on December 29, 2004. The case is still an active investigation. SA [redacted] in [redacted] is the POC. b2 b7E b6 b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

**Item #2**
**Domestic Terrorism Operations Unit (DTOU)**
**FBIHQ POC: SSA** [redacted] b6 b7C

We have had two recent investigations where we identified a victim of a computer intrusion and requested their assistance in monitoring of a computer controlled by the victim. In both cases a denial of service attack occurred using botnets and the Agents were able to identify the victim computer (server) after analyzing computers where the attack occurred. The Agents contacted the victims after determining they were not involved in the criminal act and they agreed to have sniffers attached to their computers. The purpose of this was the subject was using the victim's computer to direct or reprogram the "bots" for additional criminal activity. When the subjects logged onto the victim's computer the Agents could determine where the computer was located and direct the investigation to a new computer. This then only leads us to additional compromised computers and we start the process over to monitor the new computer.

**Item #3**
**Domestic Terrorism Operations Unit (DTOU)**
**FBIHQ POC: SSA** [redacted] (S)

DATE: 09-29-2005
CLASSIFIED BY 65179 DMH/JHF 05-CV-0845
REASON: 1.4 (C )
DECLASSIFY ON: 09-29-2030
b6 b7C

I cannot speak for whether the [redacted] were obtained based primarily upon legal changes resulting from the Patriot Act. The [redacted] investigation was conducted during the period that the Patriot Act was evolving. (S) b1 b6 b7C

General Summary:

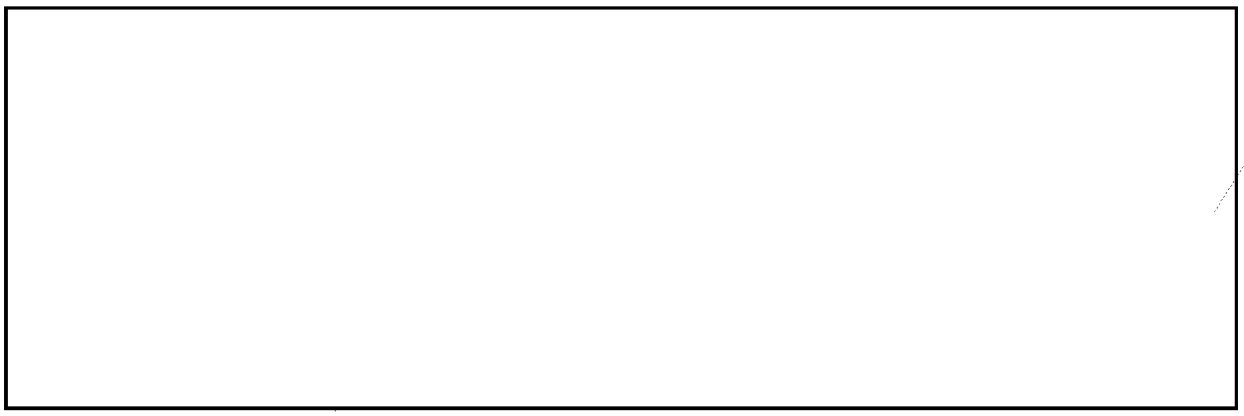
- [redacted] (S) b1 b2 b7E

- [redacted] (S)
- [redacted]
- [redacted]
- [redacted]
- [redacted]

b1
b6
b7C
b2
b7E

[redacted] (S)

b1
b6
b7C
b2
b7E



(S)

b1
b2
b7E
b6
b7C

**Item #4**
**Domestic Terrorism Operations Unit (DTOU)**
**FBIHQ POC: SSA**

b6
b7C

***Note - I believe you received this already***

In response to your e-mail disseminated to the filed, dated 03/17/2005, concerning feedback on the utility of the Patriot Act sunset provisions, after canvassing all relevant squads, responds as follows:

b2
b7E

(S) Since the inception of the Patriot Act, the JTTF (S) of use of the Expanded Title III Predicates (sections 201 and 202), Roving Wiretaps (section 206) or Computer Hacking Victims Requesting Law Enforcement Assistance (section 217). All pen registers currently and in the past three years that are being utilized by the are being done via criminal justification.

b1
b2
b7E

On November 12, 2004 the Patriot Act (section 215) was used for obtaining a National Security Letter (NSL) on a lead out of Headquarters for case In this particular instance, telephone toll records were needed on a Secret classified case and the NSL allowed lead agents to obtain the information without having to obtain a subpoena or reveal the nature of the investigation.

b7A

The most common use of the Patriot Act on the is for disseminating information in ACS that is terrorism related to state and local law enforcement (sections 203 and 218). To date, the has provided information to the National Security Bureau (NSB) of the Metropolitan Police Department on occasions. The also coordinates information sharing with BICE, the Department of Homeland Security, the US Marshals, DEA, IRS, FAM, Air Force OSI, the US Secret Service, the Attorney Generals Office, and Police Departments under the same Patriot Act sections (203 and 218).

b2
b7E

The Division has been conducting a significant Bribery, Graft and Conflicts of Interest Title 18 U.S.C. Section 201 investigation involving large amounts of money laundering. and maintained

b2
b7E
b6
b7C

corrupt relationships with [redacted] public officials designed to protect and enhance [redacted] financial interests. Due to the high profile nature of this case and the impact on [redacted] Division requested a USA Patriot Act Section 314 (a) disclosure of all banks with accounts, safe deposit boxes, and other 314(a) regarding our subjects in the case. In consultation with the Division's CDC and the United States Attorney's Office, it was decided that utilization of the Patriot Act provisions relating to money laundering would benefit the investigation. Although some publicity resulted from the requests made of the financial institutions, the resulting information was significant to the investigation. The overall outcome was positive and resulted in similar requests by other divisions to utilize the Patriot Act in non-Terrorism investigations. b6 b7C b2 b7D

We hope this feedback, when coupled with input from other field offices, will aid in our preservation of the essential sunset provisions of the Patriot Act.

**Item #5**
**Domestic Terrorism Operations Unit (DTOU)**
**FBIHQ POC: SSA [redacted]** b6 b7C

174A-OC-66039

[redacted] Comm Center received a bomb threat at 3:00 a.m. on 8/5/04. After clarifying that the bomb threat was to the local airport and that the FBI had until noon to meet the caller's demands, JTTF agents began tracing the caller id. Investigation showed the Internet was used to make the call via VoIP. The VoIP service provider provided the IP address along with the date and time of registration of the individual who was responsible for making the threat. To obtain the subscriber info to identify the individual, an emergency disclosure, as per the Patriot Act, was instituted with Comcast, the ISP used by the individual. By 7:00 a.m., a subject in [redacted] was identified. [redacted] division conducted a subject interview and the threat was determined to be non-credible by 11:00 a.m. b2 b7E

**Testimony of Robert S. Mueller, III**

**Director, Federal Bureau of Investigation**

**Before the United States Senate**

**Committee on the Judiciary**

**May 20, 2004**

---

Good morning Mr. Chairman, Senator Leahy, and Members of the Committee. I am pleased to be here today to update you on the FBI's substantial progress in the counterterrorism and intelligence arenas since my last appearance before the Committee. I would also like to acknowledge that the progress the FBI has made in reforming our counterterrorism and intelligence programs is due in no small part to the enactment of the USA PATRIOT Act.

Every day, the men and women of the FBI demonstrate their determination to fulfill the great responsibility that you, and the public, have entrusted to them. As a result, the FBI has made steady progress in meeting our highest priority of preventing terrorism. The terrorist threat presents complex challenges. Terrorists move easily across international borders, use sophisticated technology to recruit, network, and communicate, and finance their operations with elaborate funding schemes. Above all, they are patient. They are methodical. They are determined to succeed.

But the FBI is equally determined to succeed. To defeat these threats, the FBI must have several critical capabilities: First, we must develop intelligence about terrorist activity and use that intelligence to disrupt their plans. Second, we must be global – we must work closely with our counterparts at home and abroad to develop and pool our collective knowledge and expertise. Third, we must use cutting-edge information technology to collect, analyze, manage, and share our information effectively. Most importantly, we must work within the framework of the Constitution, protecting our cherished civil liberties as we work to protect the American people.

Today, I would like to give you a brief overview of the steps we have taken to put these critical capabilities in place by reforming our counterterrorism and intelligence programs, as well as overhauling our information technology. Before I begin, however, I would like to acknowledge that none of our successes would have been possible without the extraordinary efforts of our partners in state and municipal law enforcement and our counterparts around the world. The Muslim, Iraqi, and Arab-American communities have also contributed a great deal to the war on terror. On behalf of the FBI, I would like to thank these communities for their assistance and for their ongoing commitment to preventing acts of terrorism. The country owes them a debt of gratitude.

## PATRIOT ACT

Mr. Chairman, for over two and a half years, the PATRIOT Act has proved extraordinarily beneficial in the war on terrorism and has changed the way the FBI does business. Many of our counterterrorism successes, in fact, are the direct results of provisions included in the Act, a number of which are scheduled to "sunset" at the end of next year. I strongly believe it is vital to our national security to keep each of these provisions intact. Without them, the FBI could be forced back into pre-September 11 practices, attempting to fight the war on terrorism with one hand tied behind our backs.

Let me give you just a few examples that illustrate the importance of the PATRIOT Act to our counterterrorism efforts:

First and foremost, the PATRIOT Act – along with the revision of the Attorney General's investigative guidelines and the 2002 decision of the Foreign Intelligence Surveillance Court of Review – tore down the wall that stood between the intelligence investigators responding to terrorist threats and the criminal investigators responding to those same threats.

• Prior to September 11, an Agent investigating the intelligence side of a terrorism case was barred from discussing the case with an Agent across the hall who was working the criminal side of that same investigation. For instance, if a court-ordered criminal wiretap turned up intelligence information, the criminal investigator could not share that information with the intelligence investigator – he could not even suggest that the intelligence investigator should seek a wiretap to collect the information for himself. If the criminal investigator served a grand jury subpoena to a suspect's bank, he could not divulge any information found in those bank records to the intelligence investigator. Instead, the intelligence investigator would have to issue a National Security Letter in order to procure that same information.

• The removal of the "wall" has allowed government investigators to share information freely. Now, criminal investigative information that contains foreign intelligence or counterintelligence, including grand jury and wiretap information, can be shared with intelligence officials. This increased ability to share information has disrupted terrorist operations in their early stages -- such as the successful dismantling of the "Portland Seven" terror cell -- and has led to numerous arrests, prosecutions, and convictions in terrorism cases.

• In essence, prior to September 11th, criminal and intelligence investigators were attempting to put together a complex jigsaw puzzle at separate tables. The Patriot Act has fundamentally changed the way we do business. Today, those investigators sit at the same table and work together on one team. They share leads. They fuse information. Instead of conducting parallel investigations, they are fully integrated into one joint investigation.

• Because of the creation of the Terrorist Threat Integration Center, and because the FBI has dramatically improved its information sharing with the CIA, the NSA, and a host of other federal, state, local and international partners, our resources are used more effectively, our investigations are conducted more efficiently, and America is immeasurably safer as a result. We cannot afford to go back to the days when Agents and prosecutors were afraid to share information.

Second, the PATRIOT Act gave federal judges the authority to issue search warrants that are valid outside the issuing judge's district in terrorism investigations. In the past, a court could only issue a search warrant for premises within the same judicial district – yet our investigations of terrorist networks often span multiple districts. The PATRIOT Act streamlined this process, making it possible for judges in districts where activities related to terrorism may have occurred to issue search warrants applicable outside their immediate districts.

In addition, the PATRIOT Act permits similar search warrants for electronic evidence such as email. In the past, for example, if an Agent in one district needed to obtain a search warrant for a subject's email account, but the Internet service provider (ISP) was located in another district, he or she would have to contact an AUSA and Agent in the second district, brief them on the details of the investigation, and ask them to appear before a judge to obtain a search warrant – simply because the ISP was physically based in another district. Thanks to the PATRIOT Act, this frustrating and time-consuming process can be averted without reducing judicial oversight. Today, a judge anywhere in the U.S. can issue a search warrant for a subject's email, no matter where the ISP is based.

Third, the PATRIOT Act updated the law to match current technology, so that we no longer have to fight a 21st-century battle with antiquated weapons. Terrorists exploit modern technology such as the Internet and cell phones to conduct and conceal their activities. The PATRIOT Act leveled the playing field, allowing investigators to adapt to modern techniques. For example, the PATRIOT Act clarified our ability to use court-ordered pen registers and trap-and-trace devices to track Internet communications. The Act also enabled us to seek court-approved roving wiretaps, which allow investigators to conduct electronic surveillance on a particular suspect, not a particular telephone – this allows them to continuously monitor subjects without having to return to the court repeatedly for additional authorizations. This technique has long been used to investigate crimes such as drug trafficking and racketeering. In a world in which it is standard operating procedure for terrorists to rapidly change locations and switch cell phones to evade surveillance, terrorism investigators must have access to the same tools.

In a final example, the PATRIOT Act expanded our ability to pursue those who provide material support or resources to terrorist organizations. Terrorist networks rely on individuals for fund-raising, procurement of weapons and explosives, training, logistics, and recruiting. The material support statutes allow investigators to aggressively pursue and dismantle the entire terrorist network, from the financiers to those who carry out terrorist plans. By criminalizing the actions of those who provide, channel, or direct resources to terrorists, the material support statutes provide an effective tool to intervene at the earliest possible stage of terrorist planning. This allows the FBI to arrest terrorists and their supporters before their deadly plans can be carried out.

For instance, the FBI investigated a case in Charlotte, North Carolina, in which a group of Lebanese nationals purchased mass quantities of cigarettes in North Carolina and shipped them to Michigan for resale. Their scheme was highly profitable due to the cigarette tax disparity between the two states. The proceeds of their smuggling were used to fund Hezbollah affiliates and operatives in Lebanon. Similarly, the FBI investigated a case in San Diego in which subjects allegedly negotiated with undercover law enforcement officials the sale of heroin and hashish in exchange for Stinger anti-aircraft missiles, which they indicated were to be sold to Al Qaida. In both cases, the material support provisions allowed prosecutors to charge the subjects and secure guilty pleas and convictions.

Mr. Chairman and Members of the Committee, the importance of the PATRIOT Act as a valuable tool in the war against terrorism cannot be overstated. It is critical to our present and future success. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to proactively investigate and prevent terrorism and protect innocent lives, while at the same time protecting civil liberties.

## COUNTERTERRORISM AND INTELLIGENCE PROGRAM REFORMS

Let me turn for a few moments to the progress the FBI has made in strengthening and reforming its counterterrorism and intelligence programs to support its number one goal of terrorism prevention. Today, the FBI is taking full advantage of our dual role as both a law enforcement and an intelligence agency. Let me give you just a few examples of the progress we have made:

• We have more than doubled the number of counterterrorism Agents, intelligence analysts, and linguists.

• We expanded the Terrorism Financing Operations Section, which is dedicated to identifying, tracking, and cutting off terrorist funds.

• We are active participants in the Terrorist Threat Integration Center and the Terrorist Screening Center, which provides a new line of defense against terrorism by making information about known or suspected terrorists available to federal, state, and local law enforcement.

• We have worked hard to break down the walls that have sometimes hampered our coordination with our partners in federal, state and local law enforcement. Today, the FBI and CIA are integrated at virtually every level of our operations. This cooperation will be further enhanced when our Counterterrorism Division co-locates with the CIA's Counter Terrorist Center and the multi-agency Terrorist Threat Integration Center.

• We expanded the number of Joint Terrorism Task Forces (JTTF) from 34 to 84 nationwide.

• We created and refined new information sharing systems, such as the National Alert System, that electronically link us with our domestic partners.

• We have sent approximately 275 FBI executives to the Kellogg School of Management at Northwestern University to receive training on executive leadership and strategic change.

Recognizing that a strong, enterprise-wide intelligence program is critical to our success across all investigations, we have worked relentlessly to develop a strong intelligence capability and to integrate intelligence into every investigation and operation across the FBI:

• We stood up the Office of Intelligence, under the direction of a new Executive Assistant Director for Intelligence. The Office of Intelligence sets unified standards, policies, and training for analysts, who examine intelligence and ensure it is shared with our law enforcement and intelligence partners. The Office of Intelligence has already provided over 2,600 intelligence reports and other documents for the President and members of the Intelligence Community.

• We established a formal analyst training program. We are accelerating the hiring and training of analytical personnel, and developing career paths for analysts that are commensurate with their importance to the mission of the FBI.

• We developed and are in the process of executing Concepts of Operations governing all aspects of the intelligence process – from the identification of intelligence requirements to the methodology for intelligence assessment to the drafting and formatting of intelligence products.

• We established a Requirements and Collection Management Unit to identify intelligence gaps and develop collection strategies to fill those gaps.

• We established Reports Officers positions and Field Intelligence Groups in the field offices, whose members review investigative information – not only for use in investigations in that field office – but to disseminate it throughout the FBI and among our law enforcement and Intelligence Community partners.

With these changes in place, the Intelligence Program is established and growing. We are now turning to the last structural step in our effort to build an intelligence capacity. In March, I authorized new procedures governing the recruitment, training, career paths and evaluation of our Special Agents – all of which are focused on developing intelligence expertise among our agent population.

The most far-reaching of these changes will be the new agent career path, which will guarantee that agents get experience in intelligence investigations and with intelligence processes. Under this plan, new agents will spend an initial period familiarizing themselves with all aspects of the Bureau, including intelligence collection and analysis, and then go on to specialize in counterterrorism, intelligence or another operational program. A central part of this initiative will be an Intelligence Officer Certification program that will be available to both analysts and agents.

That program will be modeled after – and have the same training and experience requirements as – the existing programs in the Intelligence Community.

## INFORMATION TECHNOLOGY IMPROVEMENTS

All the progress the FBI has made on all investigative fronts rests upon a strong foundation of information technology. Over the past two and a half years, the FBI has made tremendous efforts to overhaul our information technology, and we have made significant progress.

- Over 1,000 counterterrorism and counterintelligence FBI Headquarters employees have been provided with access to Top Secret/Sensitive Compartmented Information (TS/SCI) information at their desks.
- We implemented the Wide Area Network and the Enterprise Operations Center on schedule in March 2003.

- We improved data warehousing technology to dramatically reduce stove-piping and cut down on man-hours that used to be devoted to manual searches.

- The Full Site Capability deployment began in February of this year, and was completed on April 29th. Altogether, nearly 30,000 workstations have been converted to the new Trilogy baseline software and new email system.

- We now have a permanent Chief Information Officer and Chief Technology Officer, who oversee the development and management of all IT projects and systems throughout the FBI. It is important to keep in mind that Trilogy is not the FBI's sole IT system – the FBI has over 200 IT systems, all of which must be maintained, enhanced when necessary, and certified and accredited for security.

As you know, during the past year we have encountered some setbacks regarding the deployment of Trilogy's Full Site Capability (FSC) and the Virtual Case File. Our goal is to deliver Virtual Case File capabilities by the end of this year. You are aware that last week, the National Research Council of the National Academies (NRC) released a report reviewing the Trilogy IT Modernization program. The FBI commissioned this review as part of our ongoing efforts to improve our capabilities to assemble, analyze and disseminate investigative and operational data both internally and externally with other intelligence and law enforcement agencies.

Many of the NRC's recommendations have already been implemented or are a work in progress. The FBI has repeatedly sought outside evaluation and advice throughout its IT modernization efforts and will continue to do so. The NRC report specifically noted that the counterterrorism mission requires extensive information sharing, and recommended that the FBI involve other agencies in its modernization program. We will continue to work closely with other Department of Justice Agencies and members of the Homeland Security and Intelligence Communities to ensure the FBI has the right technology to support information sharing and other mission requirements.

## CONCLUSION

With our counterterrorism, intelligence, and information technology initiatives firmly in place, the FBI is moving steadily forward, always looking for ways to evolve and improve so that we remain a step ahead of our enemies. We are looking at ways to assess and adjust our resource needs based on threats, in order to ensure that we have the personnel and resources to meet and defeat all threats.

Mr. Chairman, I would like to commend the men and women of the FBI for their hard work and dedication – dedication both to defeating terrorism and to upholding the Constitution. They have embraced and implemented the counterterrorism and intelligence reforms I have outlined for you today and they are committed to upholding their duty to protect the citizens of the United States.

Mr. Chairman, thank you again for the Committee's support of the FBI and for the opportunity to be here this morning.

I would be happy to answer any questions you might have.

b2
b6
b7A
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 113
Page 110 ~ Duplicate
Page 111 ~ Duplicate
Page 112 ~ Duplicate
Page 113 ~ Duplicate
Page 115 ~ Referral/Direct
Page 116 ~ Referral/Direct
Page 117 ~ Referral/Direct
Page 118 ~ Referral/Direct
Page 119 ~ Referral/Direct
Page 120 ~ Referral/Direct
Page 121 ~ Referral/Direct
Page 122 ~ Referral/Direct
Page 123 ~ Referral/Direct
Page 124 ~ Referral/Direct
Page 125 ~ Referral/Direct
Page 126 ~ Referral/Direct
Page 127 ~ Referral/Direct
Page 128 ~ Referral/Direct
Page 129 ~ Referral/Direct
Page 130 ~ Referral/Direct
Page 131 ~ Referral/Direct
Page 132 ~ Referral/Direct
Page 133 ~ Referral/Direct
Page 134 ~ Referral/Direct
Page 135 ~ Referral/Direct
Page 136 ~ Referral/Direct
Page 137 ~ Referral/Direct
Page 138 ~ Referral/Direct
Page 139 ~ Referral/Direct
Page 140 ~ Referral/Direct
Page 141 ~ Referral/Direct
Page 142 ~ Referral/Direct
Page 143 ~ Referral/Direct
Page 144 ~ Referral/Direct
Page 145 ~ Referral/Direct
Page 146 ~ Referral/Direct
Page 147 ~ Referral/Direct
Page 148 ~ Referral/Direct
Page 262 ~ Referral/Direct
Page 263 ~ Referral/Direct
Page 264 ~ Referral/Direct
Page 265 ~ Referral/Direct
Page 266 ~ Referral/Direct
Page 267 ~ Referral/Direct

Page 268 ~ Referral/Direct
Page 269 ~ Referral/Direct
Page 270 ~ Referral/Direct
Page 271 ~ Referral/Direct
Page 272 ~ Referral/Direct
Page 273 ~ Referral/Direct
Page 274 ~ Referral/Direct
Page 275 ~ Referral/Direct
Page 276 ~ Referral/Direct
Page 277 ~ Referral/Direct
Page 278 ~ Referral/Direct
Page 279 ~ Referral/Direct
Page 280 ~ Referral/Direct
Page 281 ~ Referral/Direct
Page 282 ~ Referral/Direct
Page 283 ~ Referral/Direct
Page 284 ~ Referral/Direct
Page 285 ~ Referral/Direct
Page 286 ~ Referral/Direct
Page 287 ~ Referral/Direct
Page 288 ~ Referral/Direct
Page 289 ~ Referral/Direct
Page 290 ~ Referral/Direct
Page 291 ~ Referral/Direct
Page 292 ~ Referral/Direct
Page 293 ~ Referral/Direct
Page 294 ~ Referral/Direct
Page 295 ~ Referral/Direct
Page 296 ~ Referral/Direct
Page 297 ~ Referral/Direct
Page 298 ~ Referral/Direct
Page 299 ~ Referral/Direct
Page 321 ~ Referral/Direct
Page 322 ~ Referral/Direct
Page 323 ~ Referral/Direct
Page 324 ~ Referral/Direct
Page 325 ~ Referral/Direct
Page 326 ~ Referral/Direct
Page 327 ~ Referral/Direct
Page 328 ~ Referral/Direct
Page 329 ~ Referral/Direct
Page 330 ~ Referral/Direct
Page 331 ~ Referral/Direct
Page 332 ~ Referral/Direct
Page 333 ~ Referral/Direct
Page 334 ~ Referral/Direct
Page 335 ~ Referral/Direct
Page 336 ~ Referral/Direct
Page 337 ~ Referral/Direct
Page 338 ~ Referral/Direct
Page 339 ~ Referral/Direct

Page 340 ~ Referral/Direct
Page 341 ~ Referral/Direct
Page 342 ~ Referral/Direct
Page 343 ~ Referral/Direct
Page 344 ~ Referral/Direct
Page 345 ~ Referral/Direct
Page 346 ~ Referral/Direct
Page 347 ~ Referral/Direct
Page 348 ~ Referral/Direct
Page 349 ~ Referral/Direct
Page 350 ~ Referral/Direct
Page 351 ~ Referral/Direct
Page 352 ~ Referral/Direct
Page 353 ~ Referral/Direct
Page 354 ~ Referral/Direct
Page 355 ~ Referral/Direct
Page 356 ~ Referral/Direct
Page 357 ~ Referral/Direct

Sunset Provisions

- On December 31, 2005, sixteen provisions of the USA PATRIOT Act are scheduled to expire. The majority of the provisions scheduled to sunset provide the FBI with investigative tools that were not available prior to September 11th and that have been critical to our success in protecting the American people. While some of the "sunset" provisions have been quite controversial, others have been subject to little criticism.

- We anticipate a spirited debate as Congress, the Executive Branch and the American people evaluate the renewal of these provisions. We are already aware of several hearings in both the House and the Senate on the various provisions. Whether FBI witnesses are testifying or we are supporting Department of Justice witnesses, we will look to the field offices to provide us with examples of how these provisions have assisted in our investigative efforts, with a particular emphasis on our efforts in the war on terror.

- I'd like to focus on the impact of the Patriot Act in a couple of key areas:

[redacted] b5

- Please send examples of success that can be attributed to Patriot Act tools to [redacted] of the Investigative Law Unit, Office of the General Counsel and to [redacted] Office of Congressional Affairs. These individuals may also contact you to respond to specific taskings.

b6

b7C

**From:** [redacted] (OCA) (FBI)
**Sent:** Friday, February 11, 2005 1:55 PM
**To:** [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (LV) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA)(FBI); [redacted] (OCA) (FBI); [redacted] (KC) (FBI); [redacted] (CTD) (FBI); [redacted] (DO) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI); [redacted] (OCA) (FBI)
**Subject:** Reauthorization of the USA Patriot Act

b6
b7C

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-13-2005 BY 65179 DMH/JHF 05-CV-0845

**UNCLASSIFIED**
**NON-RECORD**

During the 109th Congress, the Hill will be considering reauthorization of the USA Patriot Act. There are several specific provisions that will sunset unless renewed by 12/2005. In addition, there are some controversial provisions that are not scheduled to sunset, but that will be the subject of considerable debate. In anticipation of this activity, DOJ OLA has put together a USA Patriot Act working group. DOJ OLA will be closely coordinating activity through the members of the working group - I am representing FBI OCA and [redacted] is participating as a representative of FBI OGC. A couple of items of guidance are offered after the group's first meeting:

b6
b7C

1. AAG Will Moschella announced that DOJ components (including the FBI) are NOT to respond directly to any CONGRESSIONAL CORRESPONDENCE (Member, Constituent and Committee) concerning the USA Patriot Act or any of its provisions. All matters should be referred to DOJ's ExecSec. I've provided guidance to FBI ExecSec. If you receive any incoming correspondence, please forward to the FBI ExecSec for tracking and referral to DOJ. In the case of written inquiries from key members or our oversight committees, we may need to send an interim response upon referring the matter to DOJ. I will work with ExecSec if we determine interim responses are necessary.

2. DOJ OLA will be coordinating all requests for briefings or hearings on Patriot Act. [redacted] is the OLA POC if you get a request for a Patriot Act briefing or identification of a hearing witness. Please 'cc me on any e-mail to [redacted] referring a request for a briefing or hearing witness.

b6
b7C

3. Any other requests for information concerning the Patriot Act should likewise be referred to [redacted] DOJ OLA. (ie telephonic requests for comment on proposed revisions or requests for info (ie case examples) re FBI use of Patriot Act tools) Please 'cc me when referring to DOJ OLA.

b6
b7C

4. DOJ has prepared a binder of briefing material - comprised mostly of material taken from its webpage or www.lifeandliberty.com. I've provided each liaison unit chief with a copy of the binder. There is also an electronic copy of this material on the shared drive (S:/OPCA/OCA/OCAFO/Briefing Material/DOJ Patriot Act Slide Show) Click on the "start.bat" file to activate the show. This material is appropriate for dissemination to Hill staff or field office points of contact in response to general inquiries. DOJ anticipates developing additional briefing material. I will disseminate this additional material as soon as we have it.

DOJ optimistically predicts that Patriot Act reauthorization activity will begin after Easter and conclude in time for the August recess! Please reach out if you have any questions. Thanks,

[redacted]
Office of Congressional Affairs
[redacted]

b2
b6
b7C

**UNCLASSIFIED**

**From:** [redacted] (RMD) (FBI)
**Sent:** Monday, February 14, 2005 7:53 AM
**To:** [redacted] (OCA) (FBI); [redacted] (RMD) (FBI); [redacted] (RMD) (FBI)
**Cc:** KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA) (FBI)
**Subject:** RE: Correspondence re Patriot Act

b6
b7C



**UNCLASSIFIED**
**NON-RECORD**

I will inform my staff. I haven't seen any correspondence lately re: the Patriot Act, but I will let you know if I come across anything.

[redacted]-Please take note of these instructions regarding future correspondence about the Patriot Act and inform your teams.

[redacted]

b6
b7C

-----Original Message-----
**From:** [redacted] (OCA) (FBI)
**Sent:** Friday, February 11, 2005 12:58 PM
**To:** [redacted] (RMD) (FBI); ExecSec (RMD)
**Cc:** KALISCH, ELENI P. (OCA) (FBI); [redacted] (OCA) (FBI)
**Subject:** Correspondence re Patriot Act

**UNCLASSIFIED**
**NON-RECORD**

[redacted]- during the 109th Congress, the Hill will be considering reauthorization of the USA Patriot Act. It is likely that congressional interest and activity will create general public interest in this topic as well. DOJ has put together a USA Patriot Act working group. At the group's first meeting yesterday, AAG Will Moschella, DOJ Office of Legislative Affairs (OLA), announced that DOJ components (including the FBI) are NOT to respond directly to any CONGRESSIONAL CORRESPONDENCE (Member, Constituent and Committee) concerning the USA Patriot Act or any of its provisions. All matters should be referred to DOJ's ExecSec.

AD Kalisch concurs with this directive from DOJ OLA. However, in the case of written inquiries from key members or our oversight committees, we may need to send an interim response upon referring the matter to DOJ.

Please coordinate with me on these matters. I don't recall seeing any congressional correspondence concerning the Patriot Act recently - please advise if we do have any pending / assigned responses. As we begin to receive congressional correspondence - including constituent mail - please provide me with an information copy. We'll develop an interim response as appropriate depending on the nature and the volume of incoming mail.

Please call if you have any questions. Thanks,

b2
b6
b7C

[redacted]
Office of Congressional Affairs
[redacted]

**UNCLASSIFIED**

**UNCLASSIFIED**

**USA Patriot Act**
**Summary of Sunset Provisions**

The following provisions are scheduled to sunset on December 31, 2005:

**Section 201 & 202 - Expanded Title III predicates**

These provisions expanded the predicate offenses for Title III intercepts to include crimes relating to chemical weapons (18 U.S.C. § 229), terrorism (18 U.S.C. §§ 2332, 2332a, 2332b, 2332d, 2339A, and 2339B), and felony violations of computer fraud and abuse (18 U.S.C. § 1030). Later amendments to this portion of the statute expanded the Title III predicates to also include 18 U.S.C. § 2232f (Bombings of places of public use, Government facilities, public transportation systems and infrastructure facilities) and 2339C (terrorism financing). Due to the timing and statutory placement of these two additional predicate offenses, it is likely that these are now included in the sunset provision.

**Section 203 (b) & (d) - Information sharing for foreign intelligence obtained in a Title III and criminal investigations.**

Section 203(b) authorizes the sharing of foreign intelligence information obtained in a Title III electronic surveillance with other federal officials, including intelligence officers, DHS/DOD/ICE officials, and national security officials. The Homeland Security Act later authorized disclosure to foreign investigative or intelligence officials and to any federal, state, local, and foreign official when it reveals a threat of attack. The termination of the Patriot Act provision would have absurd results. It would eliminate our ability to share foreign intelligence information derived from a Title III with federal intelligence officials, while retaining the ability to share the same information with foreign intelligence officials. [redacted] b2 Only if the information constituted a threat of attack, could it be shared with federal intelligence officials.

Section 203(d) authorizes the sharing of foreign intelligence information collected in a criminal investigation with intelligence officials. The Homeland Security Act also added foreign intelligence and investigative officials to the list of receiving officials. Due to the placement of the Homeland Security Act amendments, the Congressional Research Service (CRS) has concluded that these disclosure provisions will also terminate if 203(d) is allowed to sunset.

**Section 204 - Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral and Electronic Communications**

Prior to the Patriot Act, federal statutes governing the use of criminal investigative wiretaps stated that the interception of wire or oral communications for foreign intelligence purposes should be governed by the provisions of the Foreign Intelligence Surveillance Act (FISA), rather than Title III. This provision, however, did not refer to electronic

communications. As a result, it was arguably unclear whether the interception of electronic communications, such as e-mail messages, for foreign intelligence purposes was governed by FISA or Title II (or both). Section 204 clarified the uncertainty by amending Title 18 to confirm that in foreign intelligence investigations, it is FISA, and not Title III, that governs the interception of electronic communications as well as wire and oral communications.

**Section 206 - Roving FISA Surveillance** (S)

When a FISA target's actions have the effect of thwarting surveillance, such as b[redacted] (S)
[redacted] the Court can issue an order directing as y[redacted] etc., to effect the authorized electronic surveillance. This allows the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. b1

**Section 207 - Extended Duration for Certain FISAs**

Section 207 extends the standard duration for several categories of FISA orders.

**Section 209 - Seizure of Voice Mail with a Search Warrant**

Section 209 clarified that voice mail could be obtained with a search warrant under 18 U.S.C. § 2703[redacted] Previously, some courts had required a Title III order to obtain stored voice mail. The language in Section 209 of the Patriot Act eliminated the distinction in the definitions for "wire communication" and "electronic communication" that was relied on in a 2004 First Circuit opinion (United States v. Councilman) to minimize privacy protection for e-mail. As such, should Congress allow this provision to sunset[redacted] b2 b7E b5

**Section 212 - Emergency Disclosures of E-mail & Records by ISPs**

Section 212 created a provision that allows a service provider (such as an Internet Service Provider) to voluntarily provide the content and records of communications related to a subscriber if it involves an emergency related to death or serious injury. The Homeland Security Act modified this provision as it relates to the content of communications, but not as it relates to the records held by a service provider. For this reason, the Congressional Research Service has concluded that only those provisions relating to the voluntary disclosure of records is subject to the sunset provision

**Section 214 - FISA Pen/Trap Authority**

FISA pen/trap and trace orders are now available whenever the FBI certifies that "the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." This provision eliminated the previous requirement that the application also contain specific and articulable facts giving reason to believe that the targeted line was being used by an agent of a foreign power, or was in communications with such an agent, under specified circumstances. This provision now more closely tracks the requirements to obtain a pen/trap order under the criminal provisions set forth in 18 U.S.C. § 3123. The provision also expands the FISA pen/trap to include electronic communications (i.e. Internet), comparable to the criminal pen/trap provision.

**Section 215 - Access to Business Records under FISA**

Section 215 changes the standard to compel production of business records under FISA to simple relevance (just as in the FISA pen register standard described above) and expands this authority from a limited enumerated list of certain types of business records [redacted] b2 [redacted] to include "any tangible things (including books, records, papers, b7E documents, and other items for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

**Section 217 - Interception of Computer Trespasser Communications**

The wiretap statute was amended to explicitly provide victims of computer attacks the ability to invite law enforcement into a protected computer to monitor the computer trespasser's communications. In the past, the law was ambiguous on this point and left open the possibility that a court could hold that a victim of computer hacking could not invite law enforcement in to monitor the intruder in an effort to prosecute and stop the intruder. The Patriot Act also established specific requirements and limitations that must be met before the use of this provision.

**Section 218 - Change in the "Primary Purpose" Standard of FISA**

Section 218 changed FISA to require a certification that foreign intelligence be "a significant purpose" of the authority sought. Section 504 amended FISA to allow personnel involved in a FISA to consult with law enforcement officials in order to coordinate efforts to investigate or protect against attacks, terrorism, sabotage, or clandestine intelligence activities, and that such consultation does not, in itself, undermine the required certification of "significant purpose." These changes were significant to eliminate "the wall" between criminal and intelligence investigations. They now allow FBI agents greater latitude to consult criminal

investigators or prosecutors without putting their FISAs at risk.

**Section 220 - Nationwide Search Warrants for Electronic Evidence**

Section 220 of the Act enabled courts with jurisdiction over an investigation to issue a search warrant with nationwide jurisdiction to compel the production of information held by a service provider, such as unopened e-mail. Previously, the search warrant had to be issued by a court in the district where the service provider was located. See 18 U.S.C. § 2703.

**Section 223 - Civil Liability for Certain Unauthorized Disclosures**

Prior to the passage of the Patriot Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. This section remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

**Section 225 - Immunity for Compliance with FISA Wiretap**

Pursuant to FISA, the United States may obtain wiretap or electronic surveillance orders from the FISC to monitor the communications of an entity or individual as to whom the court, among other things, finds probable cause to believe is a foreign power or the agent or a foreign power, such as international terrorists and spies. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of [redacted] to carry out such court orders. Prior to the passage of the Patriot Act, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected [redacted] assisting the government in carrying out wiretap and surveillance orders issued by the FISC under FISA. This section ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA surveillance orders, thus helping to ensure that such [redacted] will comply with orders issued by the FISC without delay.

b2
b7E

**From** [redacted] (OGC) (FBI)
**Sent:** Thursday, March 03, 2005 12:04 PM
**To** [redacted] (OCA) (FBI)
**Cc:** [redacted] (OGC) (FBI)
**Subject:** Sunset Provisions



b6
b7C

**UNCLASSIFIED**
**NON-RECORD**

[redacted] - If it is still helpful, attached please find two bullets for the Director. I focused the thoughts on information sharing and investigating internet based information for all types of crimes. The bullets emphasize the resulting impact if these provisions expire. b6 b7C

[redacted] also noted that it might be worth having the Director seek helpful examples using delayed notice search warrants, as that provision, while not a sunset provision, has come under much attack.

Finally, I did not address the FISA primary purpose standard (Section 218), but note that section's importance to the whole information sharing issue. Has anyone in OIPR (or otherwise) opined on what would happen to the FISA standard if that section were to expire? Would the FISA court's opinion be altered? Since I do not work FISA issues, I have refrained from commenting on that provision. However, I wonder if that isn't the single most important sunset provision. It might get a lot of attention if someone were to note how the landscape would change if that provision is allowed to expire.

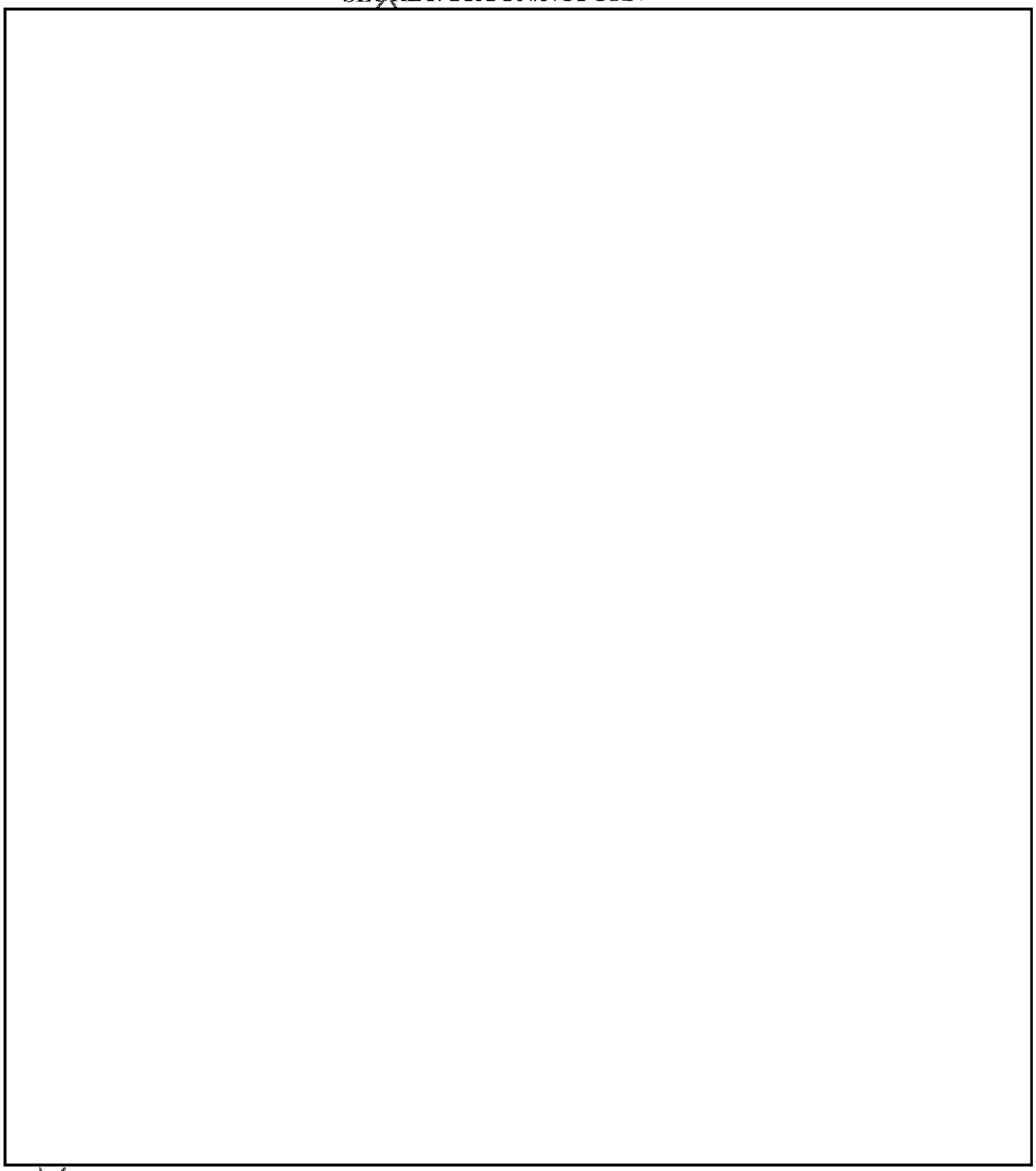
If you have any other questions, or need additional assistance on the sunset "battle," please feel free to contact me.

Thanks --

[redacted] b2
Assistant General Counsel b6
Investigative Law Unit
Office of the General Counsel b7C
[redacted]

**UNCLASSIFIED**

b5



(S/NF,OC)

b1
b7A
b6
b7C
b5

(U)

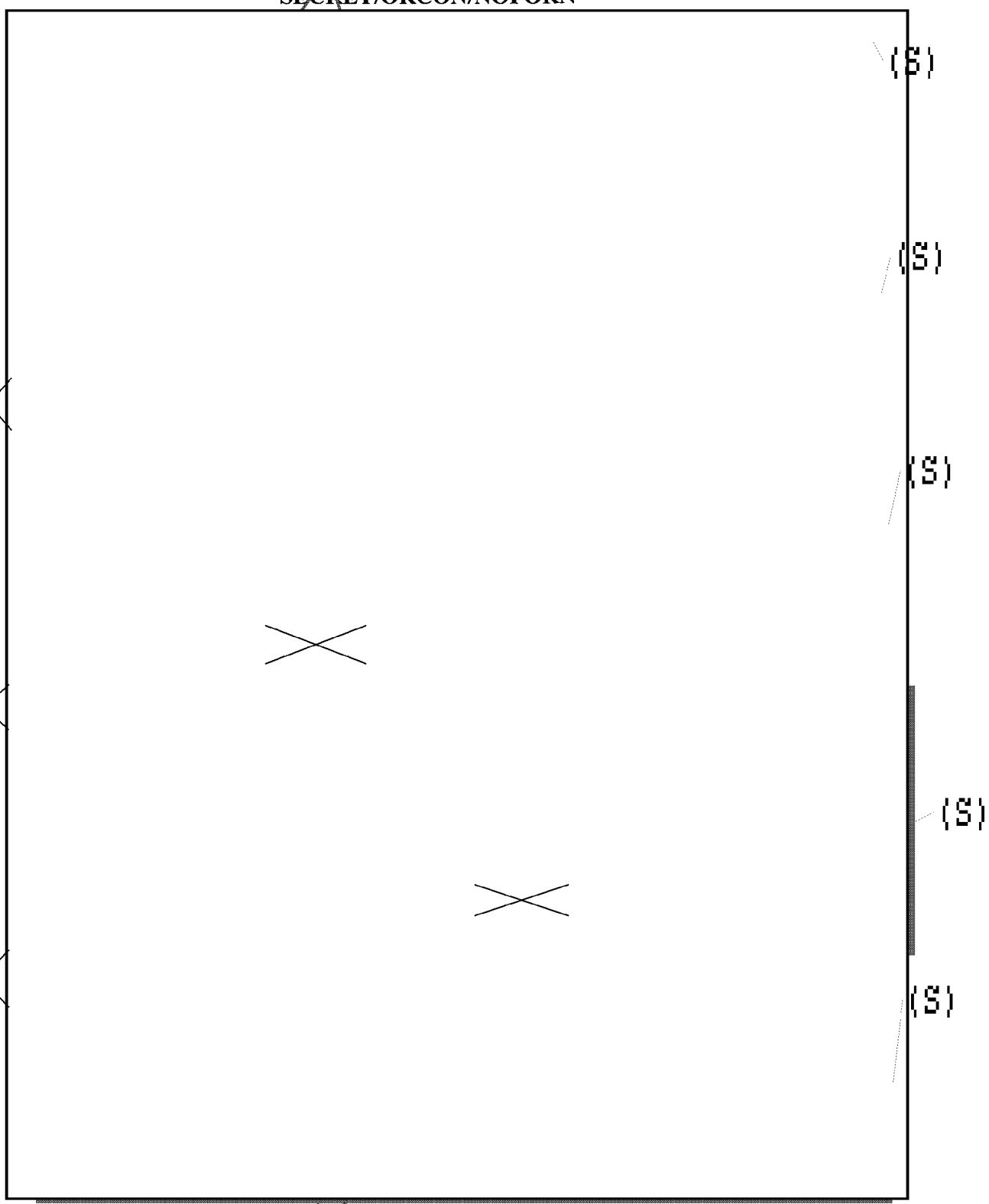
(U)

(S)

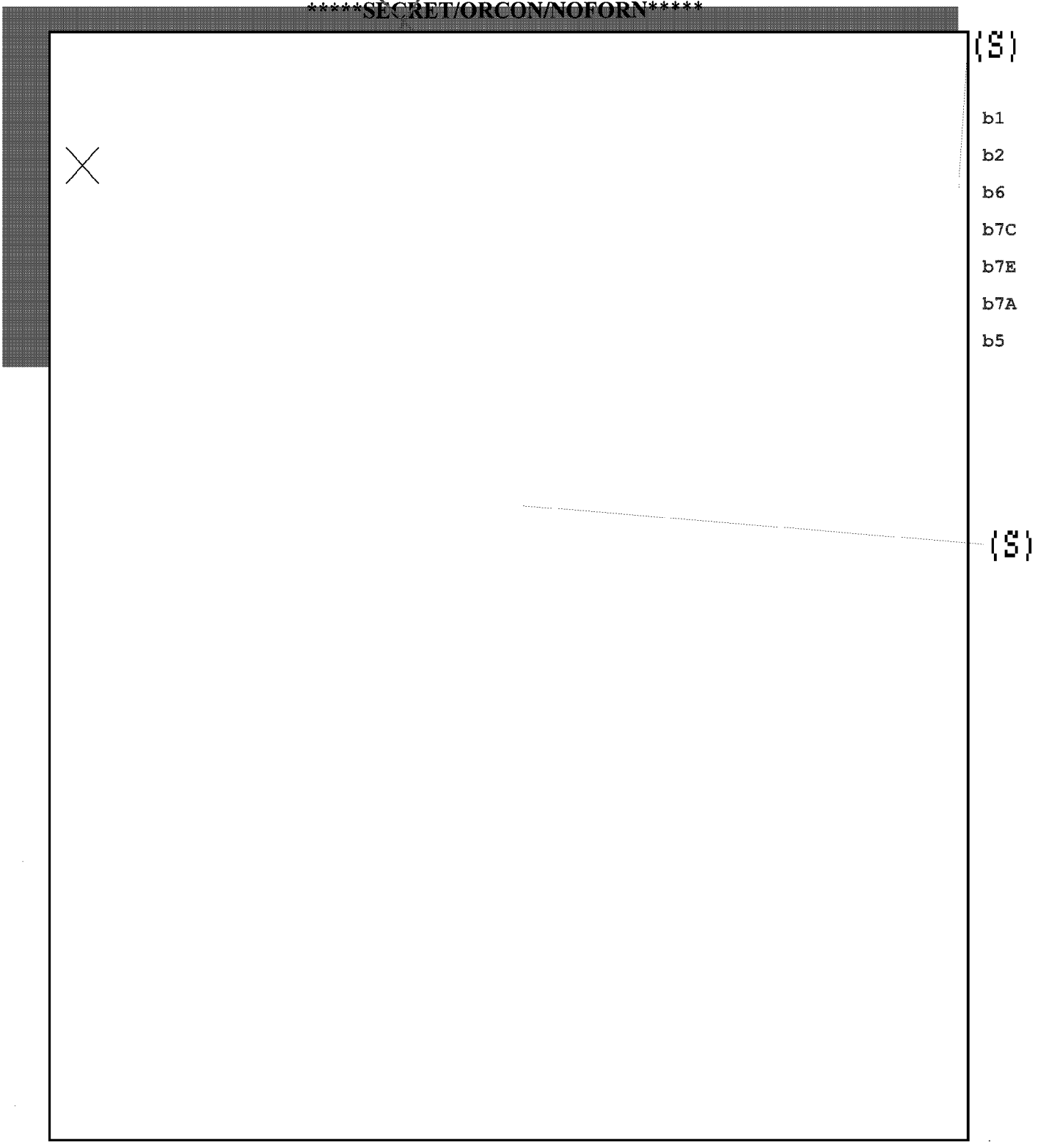
(S)

(S)

(S)



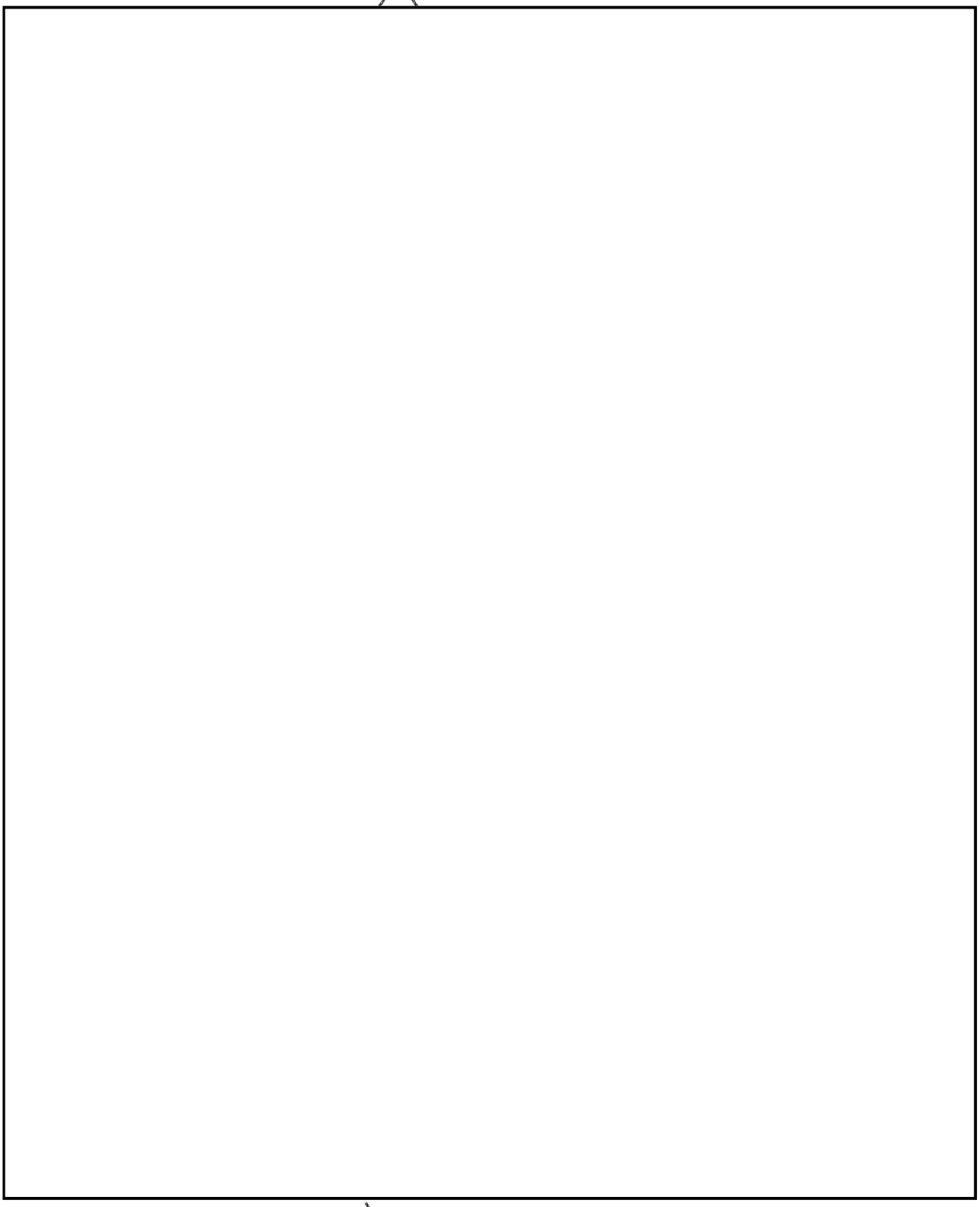

b1
b2
b5
b6
b7C
b7D
b7E
b7A



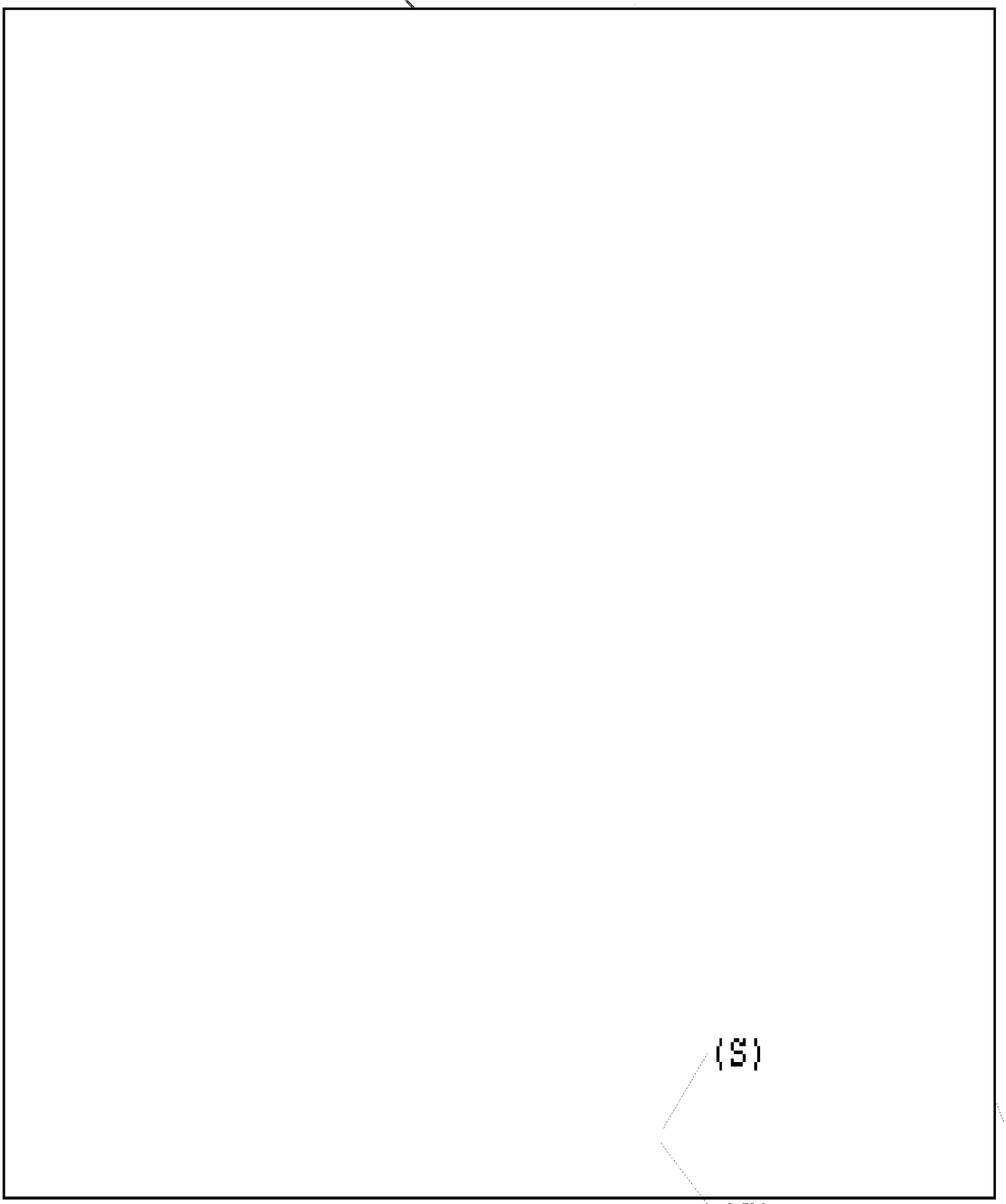
(S)

b1
b2
b6
b7C
b7E
b7A
b5

(S)



b2
b7A
b6
b7C
b5
b7E

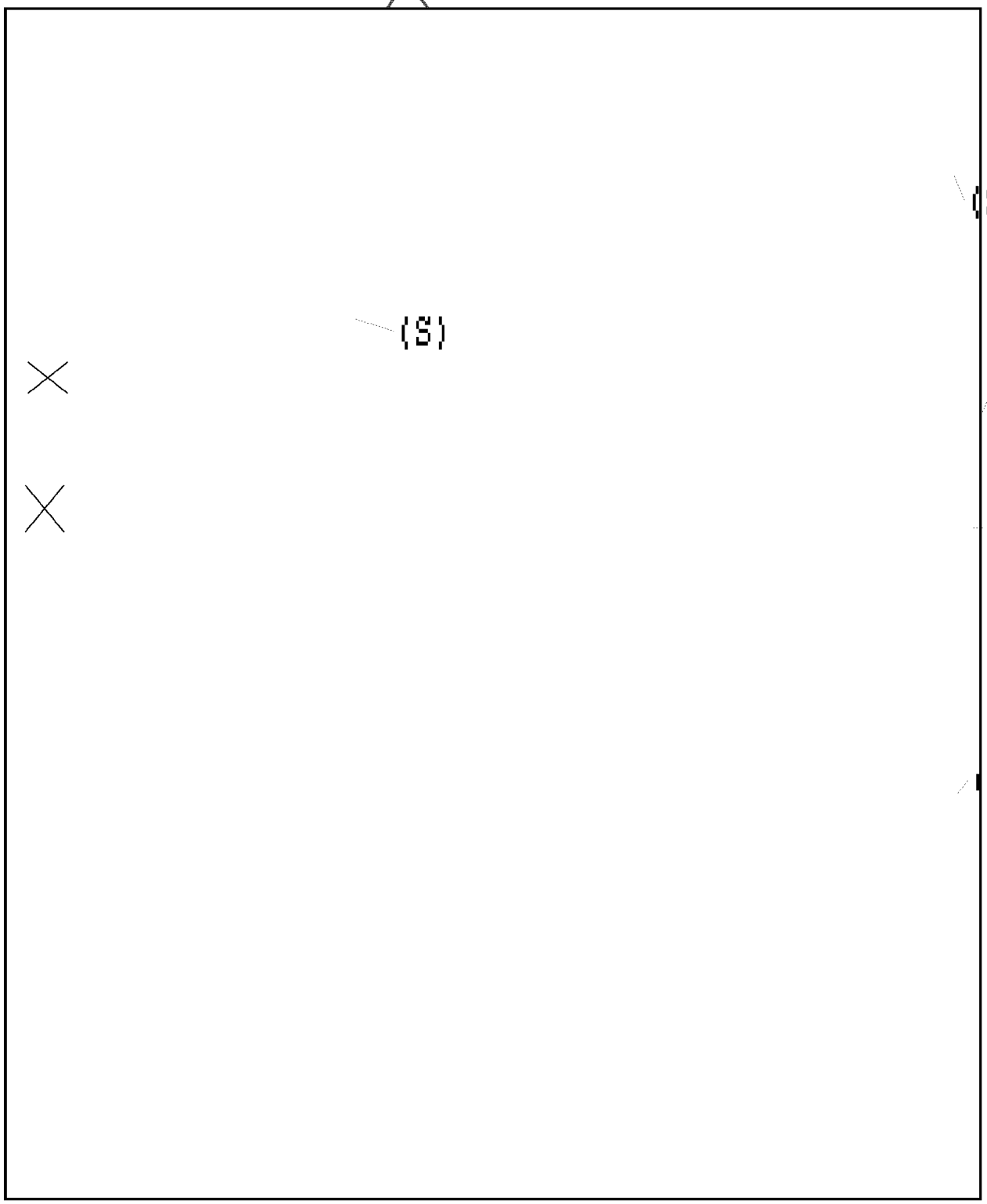


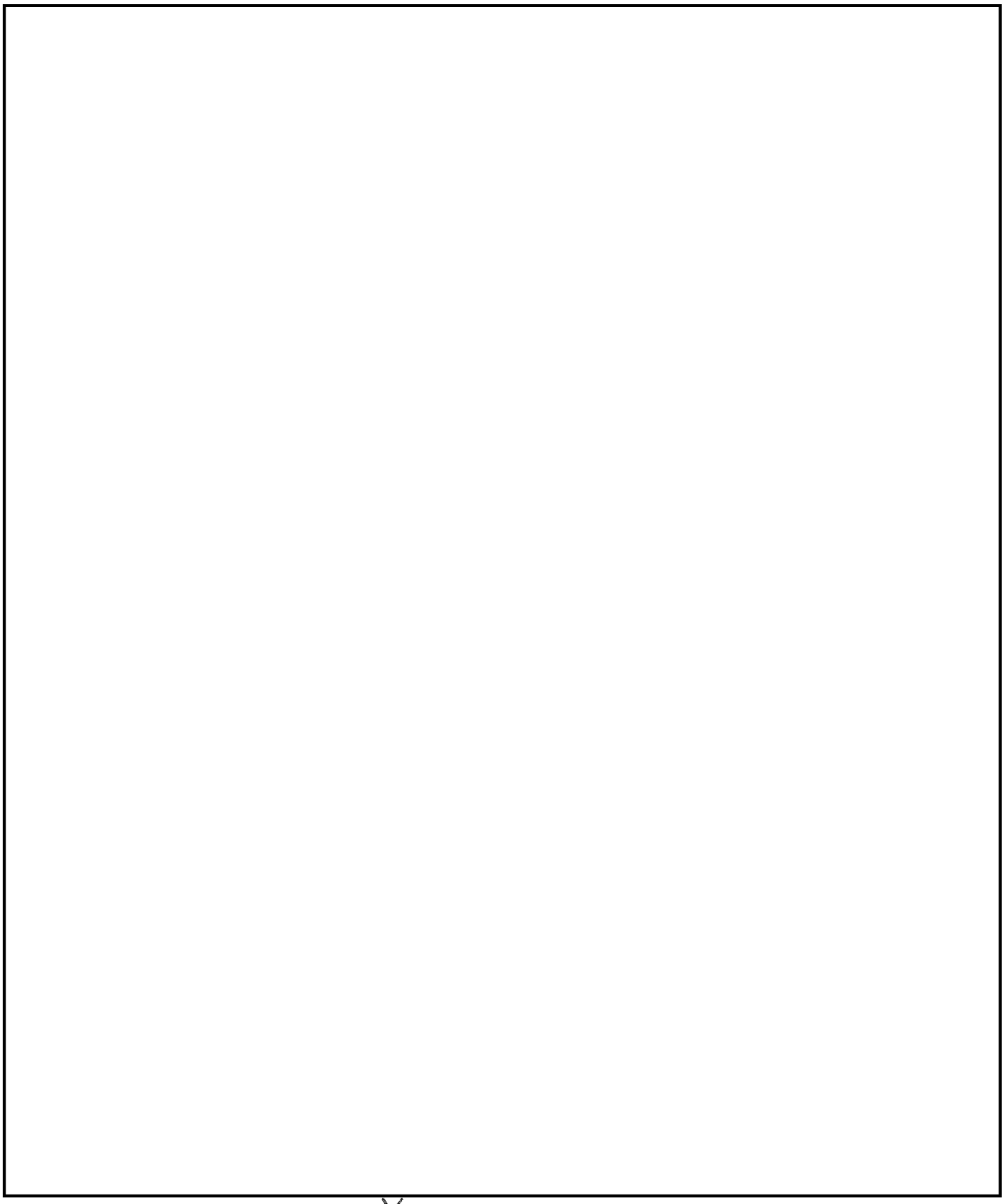
b1
b2
b6
b7A
b7C
b7E
b5

(S)

(S)

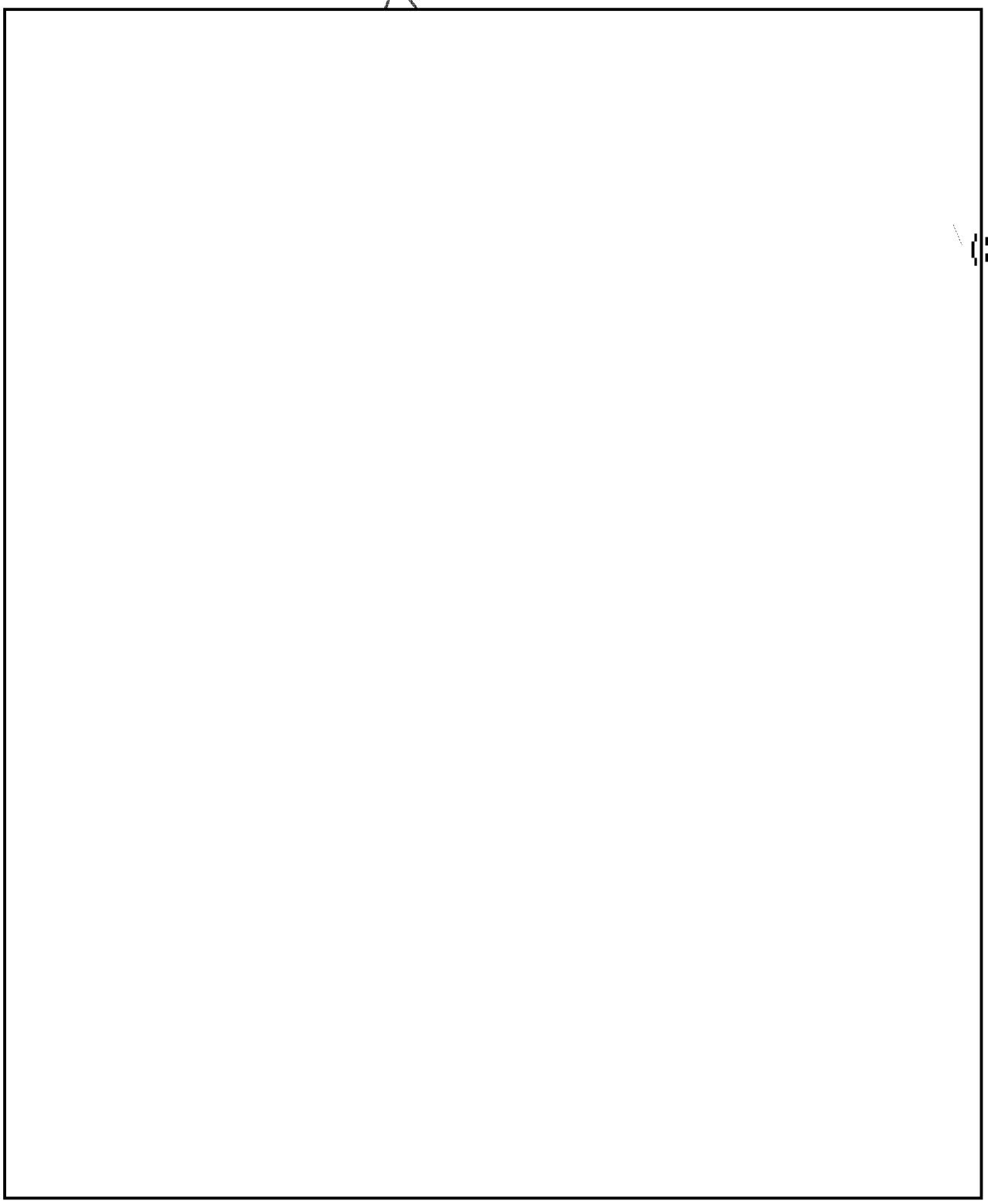
(S)


(S)
(S)
(S)
(S)
(S)
b1
b2
b5
b6
b7C
b7E



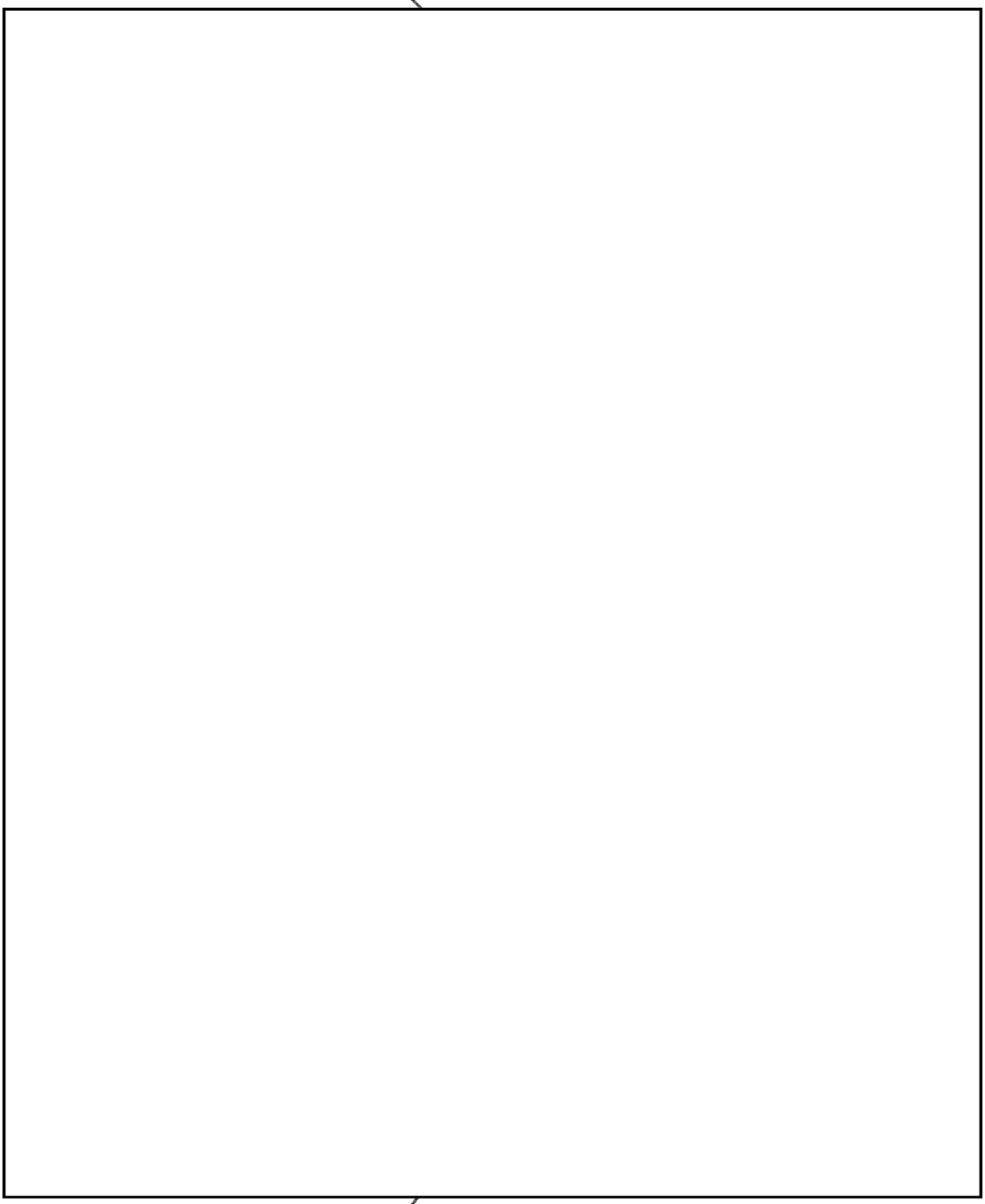
b7A

b5

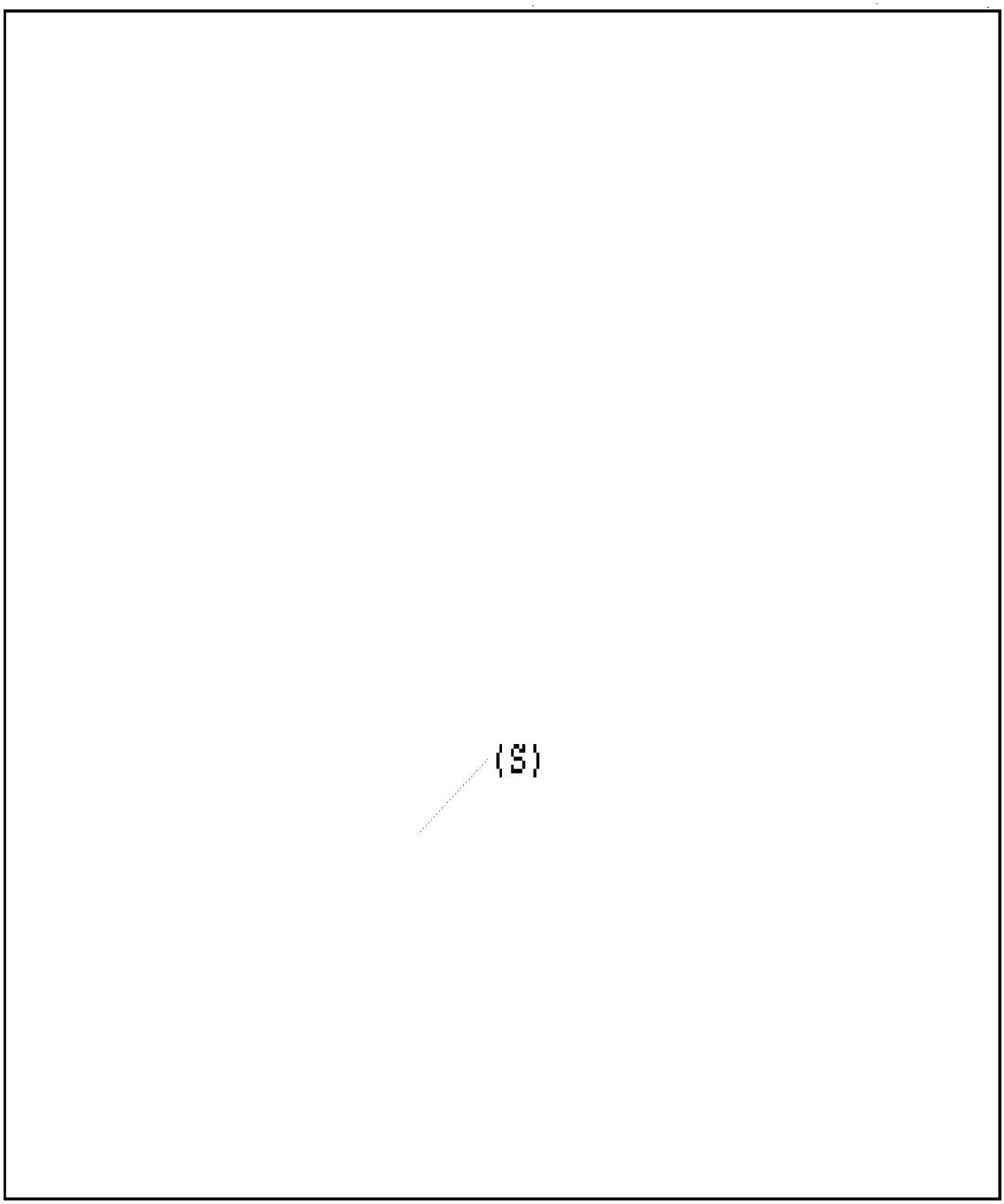


(S)

b1
b2
b7E
b5



b2
b5
b6
b7C
b7D
b7E
b7A

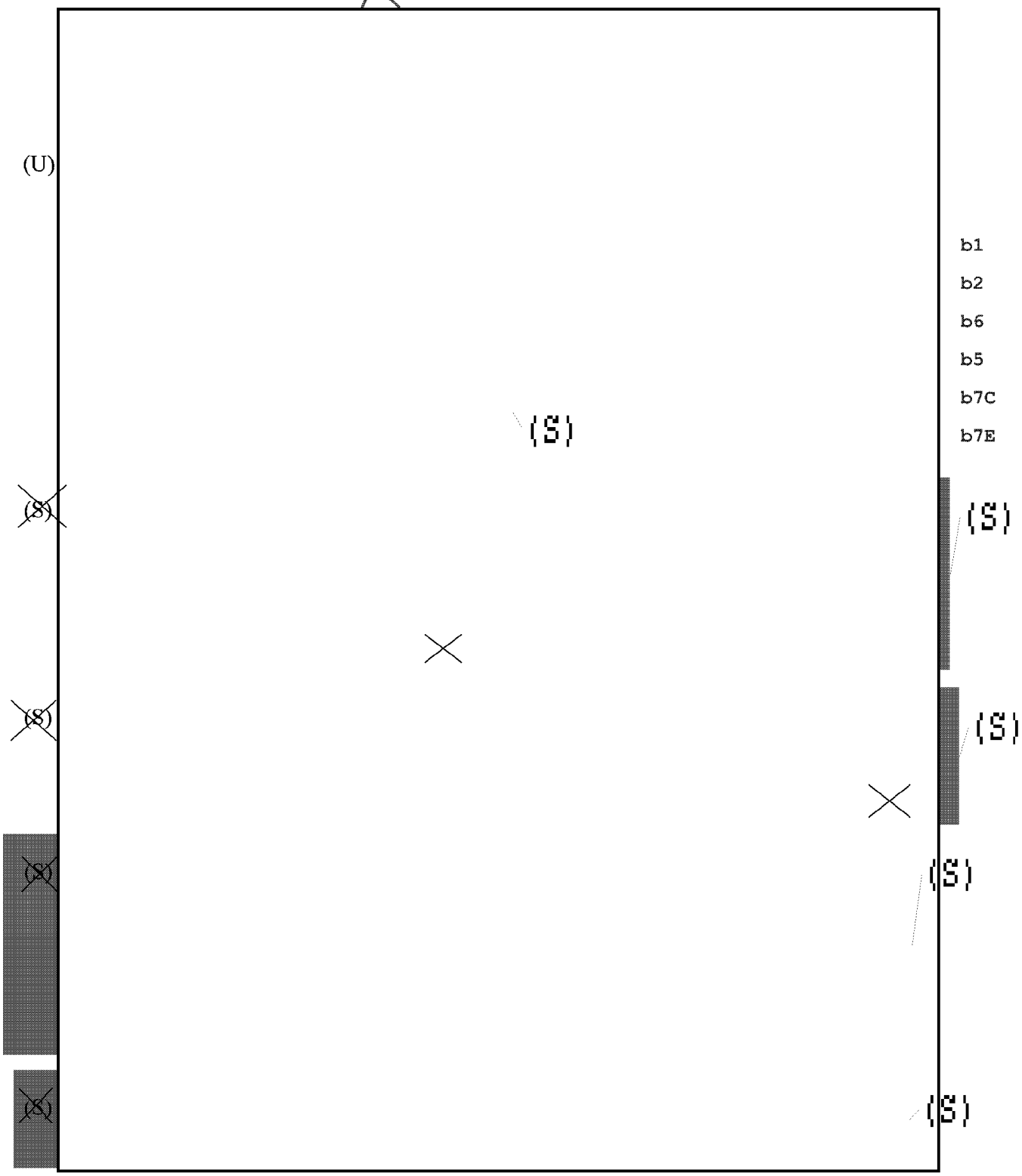


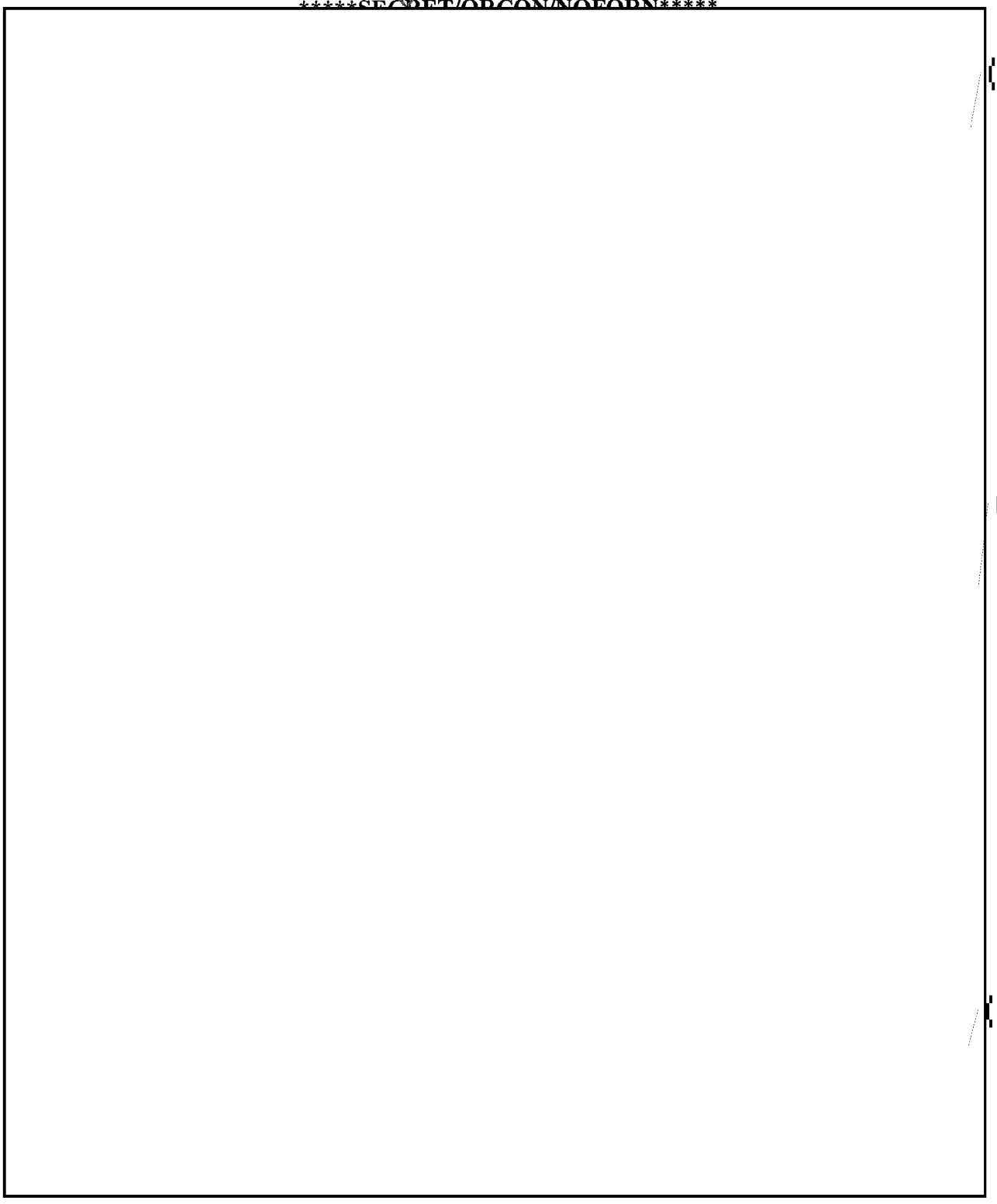
(S)

b1
b2
b7E
b6
b7C
b7A
b5

(U)

b1
b2
b6
b5
b7C
b7E





(S)

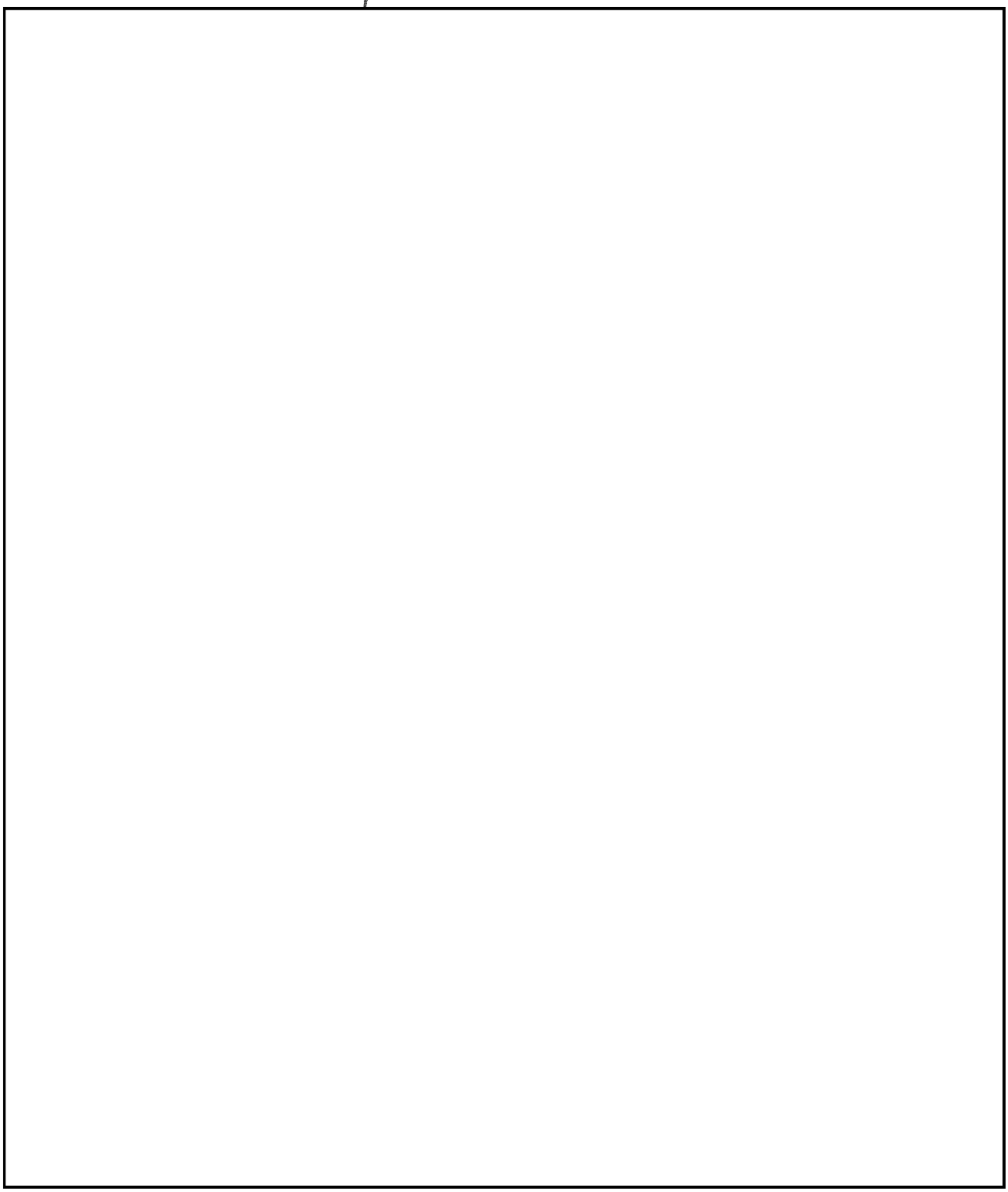
(S)

b1
b2
b5
b6
b7C
b7E

(S)

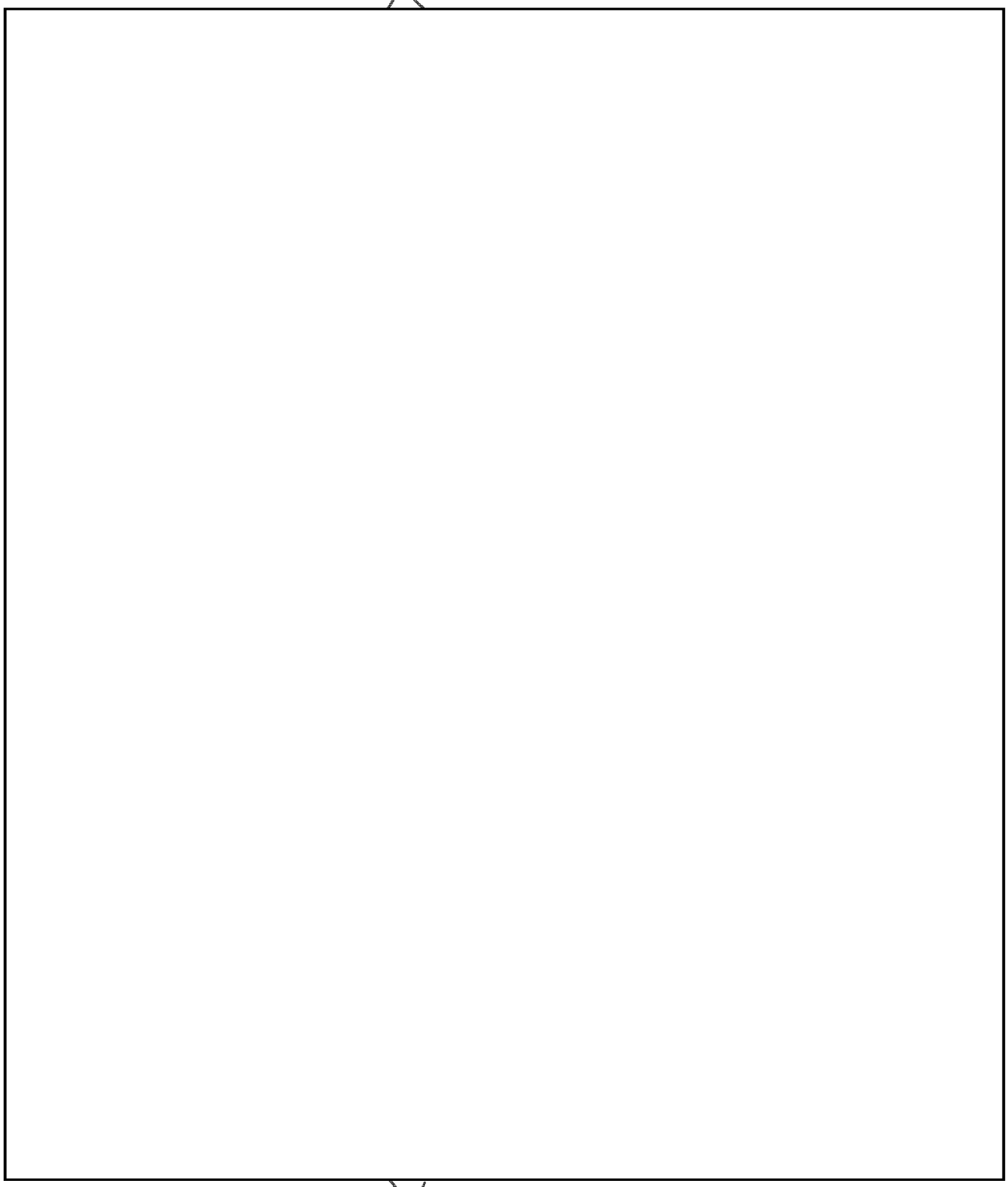
(S)

b1
b2
b7E
b5
b7A



b2
b7E
b5
b7D

b2
b7E
b7A
b6
b7C
b7D
b5



b2
b7E
b7A
b6
b7C
b7D
b5

b5
b6
b7A
b7C

(U)

(U)

(U)

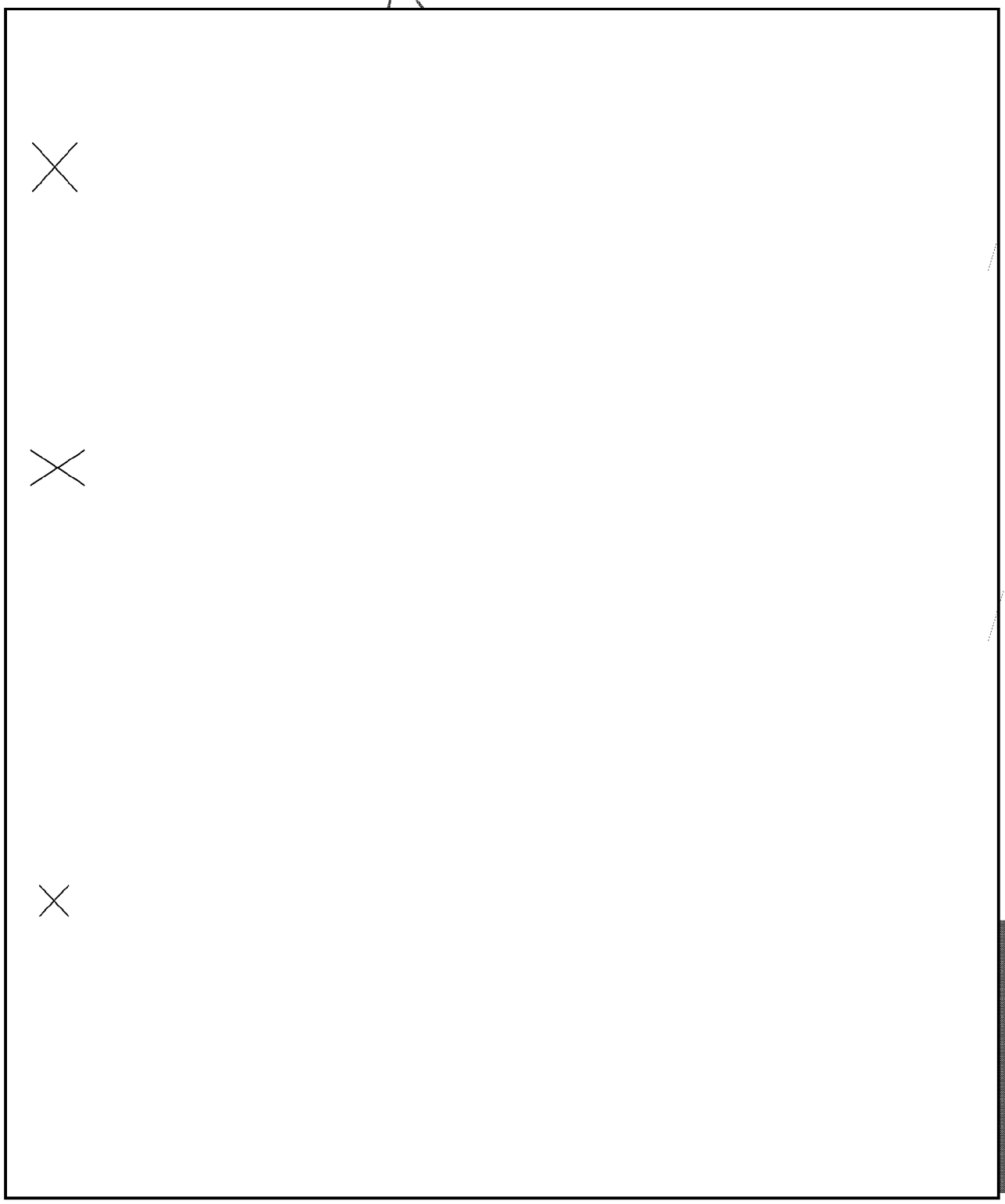
(U)

(S)

b7A

b5

b1
b2
b7E
b5



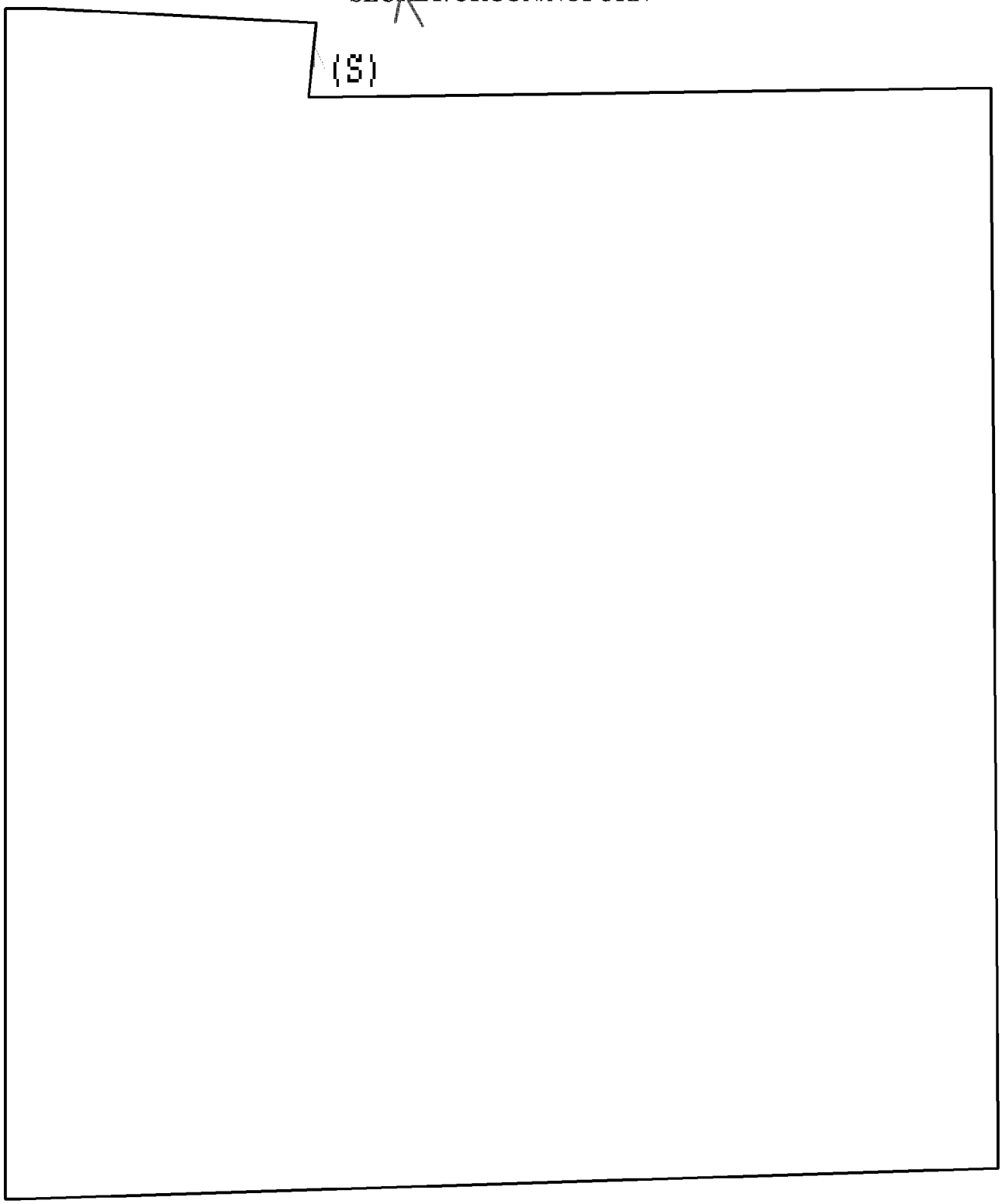
b1
b2
b7E
b5
b6
b7C
b7A

(S)

b1
b2
b5

(S)

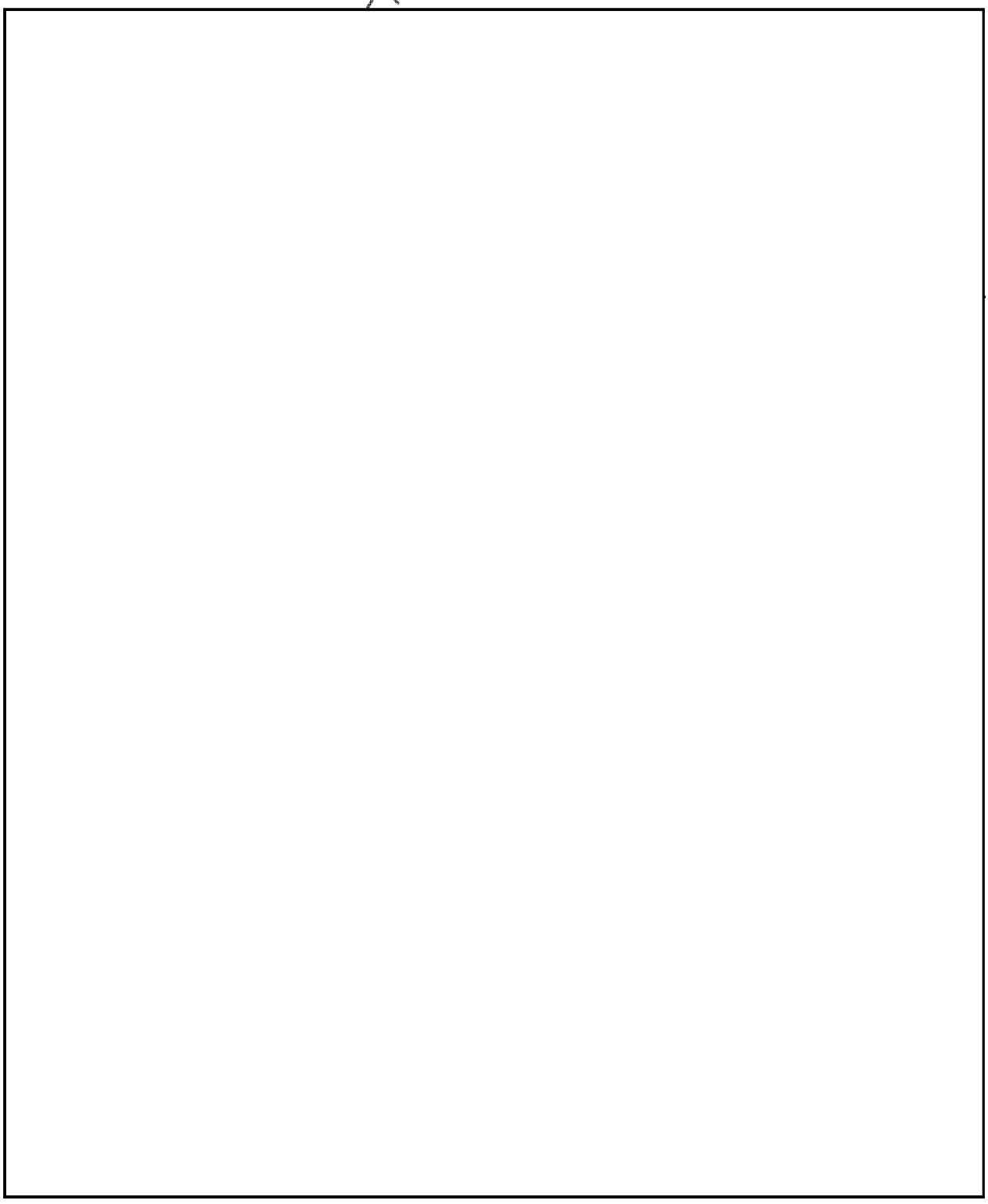
(S)



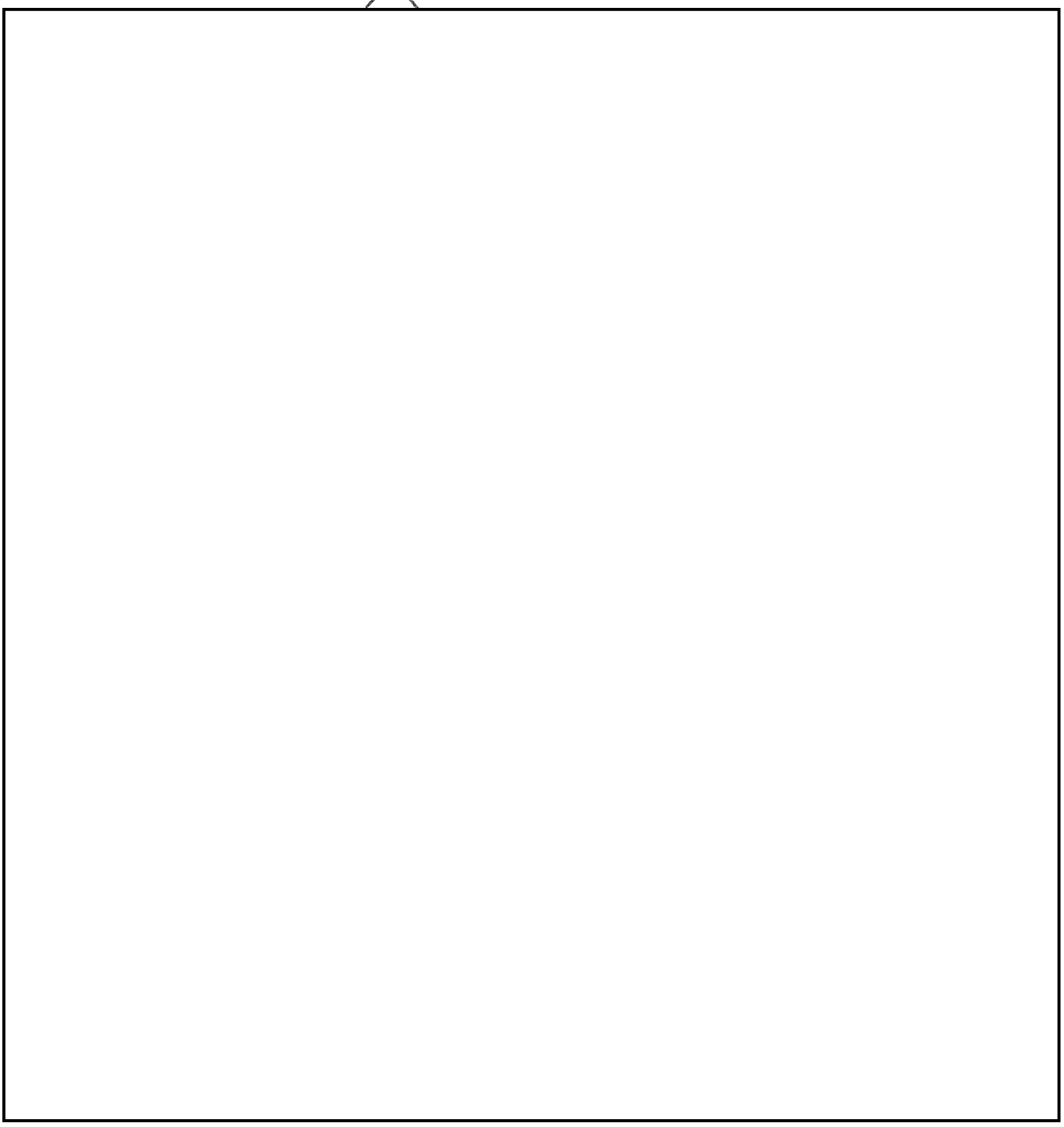
b1
b2
b7E
b5
b7A

b2
b7E
b5
b6
b7C
b7A

b5
b2
b7E
b6
b7C
b7D
b7A



b2
b7E
b6
b7C
b7A
b5



b6
b7C
b7A
b5

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 450
Page 3 ~ Referral/Direct DOJ
Page 4 ~ Referral/Direct DOJ
Page 5 ~ Referral/Direct DOJ
Page 6 ~ Referral/Direct DOJ
Page 7 ~ Referral/Direct DOJ
Page 8 ~ Referral/Direct DOJ
Page 9 ~ Referral/Direct DOJ
Page 10 ~ Referral/Direct DOJ
Page 11 ~ Referral/Direct DOJ
Page 12 ~ Referral/Direct DOJ
Page 13 ~ Referral/Direct DOJ
Page 14 ~ Referral/Direct DOJ
Page 15 ~ Referral/Direct DOJ
Page 16 ~ Referral/Direct DOJ
Page 17 ~ Referral/Direct DOJ
Page 22 ~ Referral/Direct DOJ
Page 23 ~ Referral/Direct DOJ
Page 25 ~ Referral/Direct DOJ
Page 26 ~ Referral/Direct DOJ
Page 27 ~ Referral/Direct DOJ
Page 28 ~ Referral/Direct DOJ
Page 29 ~ Referral/Direct DOJ
Page 30 ~ Referral/Direct DOJ
Page 31 ~ Referral/Direct DOJ
Page 32 ~ Referral/Direct DOJ
Page 33 ~ Referral/Direct DOJ
Page 34 ~ Referral/Direct DOJ
Page 35 ~ Referral/Direct DOJ
Page 36 ~ Referral/Direct DOJ
Page 37 ~ Referral/Direct DOJ
Page 38 ~ Referral/Direct DOJ
Page 39 ~ Referral/Direct DOJ
Page 40 ~ Referral/Direct DOJ
Page 41 ~ Referral/Direct DOJ
Page 42 ~ Referral/Direct DOJ
Page 43 ~ Referral/Direct DOJ
Page 44 ~ Referral/Direct DOJ
Page 45 ~ Referral/Direct DOJ
Page 46 ~ Referral/Direct DOJ
Page 47 ~ Referral/Direct DOJ
Page 48 ~ Referral/Direct DOJ
Page 49 ~ Referral/Direct DOJ
Page 50 ~ Referral/Direct DOJ
Page 51 ~ Referral/Direct DOJ

Page 52 ~ Referral/Direct DOJ
Page 53 ~ Referral/Direct DOJ
Page 54 ~ Referral/Direct DOJ
Page 55 ~ Referral/Direct DOJ
Page 56 ~ Referral/Direct DOJ
Page 57 ~ Referral/Direct DOJ
Page 58 ~ Referral/Direct DOJ
Page 59 ~ Referral/Direct DOJ
Page 60 ~ Referral/Direct DOJ
Page 61 ~ Referral/Direct DOJ
Page 62 ~ Referral/Direct DOJ
Page 63 ~ Referral/Direct DOJ
Page 64 ~ Referral/Direct DOJ
Page 65 ~ Referral/Direct DOJ
Page 66 ~ Referral/Direct DOJ
Page 67 ~ Referral/Direct DOJ
Page 68 ~ Referral/Direct DOJ
Page 69 ~ Referral/Direct DOJ
Page 70 ~ Referral/Direct DOJ
Page 71 ~ Referral/Direct DOJ
Page 72 ~ Referral/Direct DOJ
Page 73 ~ Referral/Direct DOJ
Page 74 ~ Referral/Direct DOJ
Page 75 ~ Referral/Direct DOJ
Page 76 ~ Referral/Direct DOJ
Page 77 ~ Referral/Direct DOJ
Page 78 ~ Referral/Direct DOJ
Page 79 ~ Referral/Direct DOJ
Page 80 ~ Referral/Direct DOJ
Page 81 ~ Referral/Direct DOJ
Page 82 ~ Referral/Direct DOJ
Page 83 ~ Referral/Direct DOJ
Page 84 ~ Referral/Direct DOJ
Page 85 ~ Referral/Direct DOJ
Page 86 ~ Referral/Direct DOJ
Page 87 ~ Referral/Direct DOJ
Page 88 ~ Referral/Direct DOJ
Page 89 ~ Referral/Direct DOJ
Page 90 ~ Referral/Direct DOJ
Page 91 ~ Referral/Direct DOJ
Page 92 ~ Referral/Direct DOJ
Page 93 ~ Referral/Direct DOJ
Page 94 ~ Referral/Direct DOJ
Page 95 ~ Referral/Direct DOJ
Page 96 ~ Referral/Direct DOJ
Page 97 ~ Referral/Direct DOJ
Page 98 ~ Referral/Direct DOJ
Page 99 ~ Referral/Direct DOJ
Page 100 ~ Referral/Direct DOJ
Page 101 ~ Referral/Direct DOJ
Page 102 ~ Referral/Direct DOJ

Page 103 ~ Referral/Direct DOJ
Page 104 ~ Referral/Direct DOJ
Page 105 ~ Referral/Direct DOJ
Page 106 ~ Referral/Direct DOJ
Page 107 ~ Referral/Direct DOJ
Page 108 ~ Referral/Direct DOJ
Page 109 ~ Referral/Direct DOJ
Page 110 ~ Referral/Direct DOJ
Page 111 ~ Referral/Direct DOJ
Page 112 ~ Referral/Direct DOJ
Page 113 ~ Referral/Direct DOJ
Page 114 ~ Referral/Direct DOJ
Page 115 ~ Referral/Direct DOJ
Page 116 ~ Referral/Direct DOJ
Page 117 ~ Referral/Direct DOJ
Page 118 ~ Referral/Direct DOJ
Page 119 ~ Referral/Direct DOJ
Page 120 ~ Referral/Direct DOJ
Page 121 ~ Referral/Direct DOJ
Page 122 ~ Referral/Direct DOJ
Page 123 ~ Referral/Direct DOJ
Page 124 ~ Referral/Direct DOJ
Page 125 ~ Referral/Direct DOJ
Page 126 ~ Referral/Direct DOJ
Page 127 ~ Referral/Direct DOJ
Page 128 ~ Referral/Direct DOJ
Page 129 ~ Referral/Direct DOJ
Page 130 ~ Referral/Direct DOJ
Page 131 ~ Referral/Direct DOJ
Page 132 ~ Referral/Direct DOJ
Page 133 ~ Referral/Direct DOJ
Page 134 ~ Referral/Direct DOJ
Page 135 ~ Referral/Direct DOJ
Page 136 ~ Referral/Direct DOJ
Page 137 ~ Referral/Direct DOJ
Page 138 ~ Referral/Direct DOJ
Page 139 ~ Referral/Direct DOJ
Page 140 ~ Referral/Direct DOJ
Page 141 ~ Referral/Direct DOJ
Page 142 ~ Referral/Direct DOJ
Page 143 ~ Referral/Direct DOJ
Page 144 ~ Referral/Direct DOJ
Page 145 ~ Referral/Direct DOJ
Page 146 ~ Referral/Direct DOJ
Page 147 ~ Referral/Direct DOJ
Page 148 ~ Referral/Direct DOJ
Page 149 ~ Referral/Direct DOJ
Page 150 ~ Referral/Direct DOJ
Page 151 ~ Referral/Direct DOJ
Page 152 ~ Referral/Direct DOJ
Page 153 ~ Referral/Direct DOJ

Page 154 ~ Referral/Direct DOJ
Page 155 ~ Referral/Direct DOJ
Page 156 ~ Referral/Direct DOJ
Page 157 ~ Referral/Direct DOJ
Page 158 ~ Referral/Direct DOJ
Page 159 ~ Referral/Direct DOJ
Page 160 ~ Referral/Direct DOJ
Page 161 ~ Referral/Direct DOJ
Page 162 ~ Referral/Direct DOJ
Page 163 ~ Referral/Direct DOJ
Page 164 ~ Referral/Direct DOJ
Page 165 ~ Referral/Direct DOJ
Page 166 ~ Referral/Direct DOJ
Page 167 ~ Referral/Direct DOJ
Page 168 ~ Referral/Direct DOJ
Page 169 ~ Referral/Direct DOJ
Page 170 ~ Referral/Direct DOJ
Page 171 ~ Referral/Direct DOJ
Page 172 ~ Referral/Direct DOJ
Page 173 ~ Referral/Direct DOJ
Page 174 ~ Referral/Direct DOJ
Page 175 ~ Referral/Direct DOJ
Page 176 ~ Referral/Direct DOJ
Page 177 ~ Referral/Direct DOJ
Page 178 ~ Referral/Direct DOJ
Page 179 ~ Referral/Direct DOJ
Page 180 ~ Referral/Direct DOJ
Page 181 ~ Referral/Direct DOJ
Page 182 ~ Referral/Direct DOJ
Page 183 ~ Referral/Direct DOJ
Page 184 ~ Referral/Direct DOJ
Page 185 ~ Referral/Direct DOJ
Page 186 ~ Referral/Direct DOJ
Page 187 ~ Referral/Direct DOJ
Page 188 ~ Referral/Direct DOJ
Page 189 ~ Referral/Direct DOJ
Page 190 ~ Referral/Direct DOJ
Page 191 ~ Referral/Direct DOJ
Page 192 ~ Referral/Direct DOJ
Page 193 ~ Referral/Direct DOJ
Page 194 ~ Referral/Direct DOJ
Page 195 ~ Referral/Direct DOJ
Page 196 ~ Referral/Direct DOJ
Page 197 ~ Referral/Direct DOJ
Page 198 ~ Referral/Direct DOJ
Page 199 ~ Referral/Direct DOJ
Page 200 ~ Referral/Direct DOJ
Page 201 ~ Referral/Direct DOJ
Page 202 ~ Referral/Direct DOJ
Page 203 ~ Referral/Direct DOJ
Page 204 ~ Referral/Direct DOJ

Page 205 ~ Referral/Direct DOJ
Page 206 ~ Referral/Direct DOJ
Page 207 ~ Referral/Direct DOJ
Page 208 ~ Referral/Direct DOJ
Page 209 ~ Referral/Direct DOJ
Page 210 ~ Referral/Direct DOJ
Page 211 ~ Referral/Direct DOJ
Page 212 ~ Referral/Direct DOJ
Page 213 ~ Referral/Direct DOJ
Page 214 ~ Referral/Direct DOJ
Page 215 ~ Referral/Direct DOJ
Page 216 ~ Referral/Direct DOJ
Page 217 ~ Referral/Direct DOJ
Page 218 ~ Referral/Direct DOJ
Page 219 ~ Referral/Direct DOJ
Page 220 ~ Referral/Direct DOJ
Page 221 ~ Referral/Direct DOJ
Page 222 ~ Referral/Direct DOJ
Page 223 ~ Referral/Direct DOJ
Page 224 ~ Referral/Direct DOJ
Page 225 ~ Referral/Direct DOJ
Page 226 ~ Referral/Direct DOJ
Page 227 ~ Referral/Direct DOJ
Page 228 ~ Referral/Direct DOJ
Page 229 ~ Referral/Direct DOJ
Page 230 ~ Referral/Direct DOJ
Page 231 ~ Referral/Direct DOJ
Page 232 ~ Referral/Direct DOJ
Page 233 ~ Referral/Direct DOJ
Page 234 ~ Referral/Direct DOJ
Page 235 ~ Referral/Direct DOJ
Page 236 ~ Referral/Direct DOJ
Page 237 ~ Referral/Direct DOJ
Page 238 ~ Referral/Direct DOJ
Page 239 ~ Referral/Direct DOJ
Page 240 ~ Referral/Direct DOJ
Page 241 ~ Referral/Direct DOJ
Page 242 ~ Referral/Direct DOJ
Page 243 ~ Referral/Direct DOJ
Page 244 ~ Referral/Direct DOJ
Page 245 ~ Referral/Direct DOJ
Page 246 ~ Referral/Direct DOJ
Page 247 ~ Referral/Direct DOJ
Page 248 ~ Referral/Direct DOJ
Page 249 ~ Referral/Direct DOJ
Page 250 ~ Referral/Direct DOJ
Page 251 ~ Referral/Direct DOJ
Page 252 ~ Referral/Direct DOJ
Page 253 ~ Referral/Direct DOJ
Page 254 ~ Referral/Direct DOJ
Page 255 ~ Referral/Direct DOJ

Page 256 ~ Referral/Direct DOJ
Page 257 ~ Referral/Direct DOJ
Page 258 ~ Referral/Direct DOJ
Page 259 ~ Referral/Direct DOJ
Page 260 ~ Referral/Direct DOJ
Page 261 ~ Referral/Direct DOJ
Page 262 ~ Referral/Direct DOJ
Page 263 ~ Referral/Direct DOJ
Page 264 ~ Referral/Direct DOJ
Page 265 ~ Referral/Direct DOJ
Page 266 ~ Referral/Direct DOJ
Page 267 ~ Referral/Direct DOJ
Page 268 ~ Referral/Direct DOJ
Page 269 ~ Referral/Direct DOJ
Page 270 ~ Referral/Direct DOJ
Page 271 ~ Referral/Direct DOJ
Page 272 ~ Referral/Direct DOJ
Page 273 ~ Referral/Direct DOJ
Page 274 ~ Referral/Direct DOJ
Page 275 ~ Referral/Direct DOJ
Page 276 ~ Referral/Direct DOJ
Page 277 ~ Referral/Direct DOJ
Page 278 ~ Referral/Direct DOJ
Page 279 ~ Referral/Direct DOJ
Page 280 ~ Referral/Direct DOJ
Page 281 ~ Referral/Direct DOJ
Page 282 ~ Referral/Direct DOJ
Page 283 ~ Referral/Direct DOJ
Page 284 ~ Referral/Direct DOJ
Page 285 ~ Referral/Direct DOJ
Page 286 ~ Referral/Direct DOJ
Page 287 ~ Referral/Direct DOJ
Page 288 ~ Referral/Direct DOJ
Page 289 ~ Referral/Direct DOJ
Page 290 ~ Referral/Direct DOJ
Page 291 ~ Referral/Direct DOJ
Page 292 ~ Referral/Direct DOJ
Page 293 ~ Referral/Direct DOJ
Page 294 ~ Referral/Direct DOJ
Page 295 ~ Referral/Direct DOJ
Page 296 ~ Referral/Direct DOJ
Page 297 ~ Referral/Direct DOJ
Page 298 ~ Referral/Direct DOJ
Page 299 ~ Referral/Direct DOJ
Page 300 ~ Referral/Direct DOJ
Page 301 ~ Referral/Direct DOJ
Page 302 ~ Referral/Direct DOJ
Page 303 ~ Referral/Direct DOJ
Page 304 ~ Referral/Direct DOJ
Page 305 ~ Referral/Direct DOJ
Page 306 ~ Referral/Direct DOJ

Page 307 ~ Referral/Direct DOJ
Page 308 ~ Referral/Direct DOJ
Page 309 ~ Referral/Direct DOJ
Page 310 ~ Referral/Direct DOJ
Page 311 ~ Referral/Direct DOJ
Page 312 ~ Referral/Direct DOJ
Page 313 ~ Referral/Direct DOJ
Page 314 ~ Referral/Direct DOJ
Page 315 ~ Referral/Direct DOJ
Page 316 ~ Referral/Direct DOJ
Page 317 ~ Referral/Direct DOJ
Page 318 ~ Referral/Direct DOJ
Page 319 ~ Referral/Direct DOJ
Page 320 ~ Referral/Direct DOJ
Page 321 ~ Referral/Direct DOJ
Page 322 ~ Referral/Direct DOJ
Page 323 ~ Referral/Direct DOJ
Page 324 ~ Referral/Direct DOJ
Page 325 ~ Referral/Direct DOJ
Page 388 ~ Referral/Direct DOJ (pages 388-453)
Page 389 ~ Referral/Direct DOJ (pages 388-453)
Page 390 ~ Referral/Direct DOJ (pages 388-453)
Page 391 ~ Referral/Direct DOJ (pages 388-453)
Page 392 ~ Referral/Direct DOJ (pages 388-453)
Page 393 ~ Referral/Direct DOJ (pages 388-453)
Page 394 ~ Referral/Direct DOJ (pages 388-453)
Page 395 ~ Referral/Direct DOJ (pages 388-453)
Page 396 ~ Referral/Direct DOJ (pages 388-453)
Page 397 ~ Referral/Direct DOJ (pages 388-453)
Page 398 ~ Referral/Direct DOJ (pages 388-453)
Page 399 ~ Referral/Direct DOJ (pages 388-453)
Page 400 ~ Referral/Direct DOJ (pages 388-453)
Page 401 ~ Referral/Direct DOJ (pages 388-453)
Page 402 ~ Referral/Direct DOJ (pages 388-453)
Page 403 ~ Referral/Direct DOJ (pages 388-453)
Page 404 ~ Referral/Direct DOJ (pages 388-453)
Page 405 ~ Referral/Direct DOJ (pages 388-453)
Page 406 ~ Referral/Direct DOJ (pages 388-453)
Page 407 ~ Referral/Direct DOJ (pages 388-453)
Page 408 ~ Referral/Direct DOJ (pages 388-453)
Page 409 ~ Referral/Direct DOJ (pages 388-453)
Page 410 ~ Referral/Direct DOJ (pages 388-453)
Page 411 ~ Referral/Direct DOJ (pages 388-453)
Page 412 ~ Referral/Direct DOJ (pages 388-453)
Page 413 ~ Referral/Direct DOJ (pages 388-453)
Page 414 ~ Referral/Direct DOJ (pages 388-453)
Page 415 ~ Referral/Direct DOJ (pages 388-453)
Page 416 ~ Referral/Direct DOJ (pages 388-453)
Page 417 ~ Referral/Direct DOJ (pages 388-453)
Page 418 ~ Referral/Direct DOJ (pages 388-453)
Page 419 ~ Referral/Direct DOJ (pages 388-453)

Page 420 ~ Referral/Direct DOJ (pages 388-453)
Page 421 ~ Referral/Direct DOJ (pages 388-453)
Page 422 ~ Referral/Direct DOJ (pages 388-453)
Page 423 ~ Referral/Direct DOJ (pages 388-453)
Page 424 ~ Referral/Direct DOJ (pages 388-453)
Page 425 ~ Referral/Direct DOJ (pages 388-453)
Page 426 ~ Referral/Direct DOJ (pages 388-453)
Page 427 ~ Referral/Direct DOJ (pages 388-453)
Page 428 ~ Referral/Direct DOJ (pages 388-453)
Page 429 ~ Referral/Direct DOJ (pages 388-453)
Page 430 ~ Referral/Direct DOJ (pages 388-453)
Page 431 ~ Referral/Direct DOJ (pages 388-453)
Page 432 ~ Referral/Direct DOJ (pages 388-453)
Page 433 ~ Referral/Direct DOJ (pages 388-453)
Page 434 ~ Referral/Direct DOJ (pages 388-453)
Page 435 ~ Referral/Direct DOJ (pages 388-453)
Page 436 ~ Referral/Direct DOJ (pages 388-453)
Page 437 ~ Referral/Direct DOJ (pages 388-453)
Page 438 ~ Referral/Direct DOJ (pages 388-453)
Page 439 ~ Referral/Direct DOJ (pages 388-453)
Page 440 ~ Referral/Direct DOJ (pages 388-453)
Page 441 ~ Referral/Direct DOJ (pages 388-453)
Page 442 ~ Referral/Direct DOJ (pages 388-453)
Page 443 ~ Referral/Direct DOJ (pages 388-453)
Page 444 ~ Referral/Direct DOJ (pages 388-453)
Page 445 ~ Referral/Direct DOJ (pages 388-453)
Page 446 ~ Referral/Direct DOJ (pages 388-453)
Page 447 ~ Referral/Direct DOJ (pages 388-453)
Page 448 ~ Referral/Direct DOJ (pages 388-453)
Page 449 ~ Referral/Direct DOJ (pages 388-453)
Page 450 ~ Referral/Direct DOJ (pages 388-453)
Page 451 ~ Referral/Direct DOJ (pages 388-453)
Page 452 ~ Referral/Direct DOJ (pages 388-453)
Page 453 ~ Referral/Direct DOJ (pages 388-453)
Page 454 ~ Referral/Direct DOJ
Page 455 ~ Referral/Direct DOJ
Page 456 ~ Referral/Direct DOJ
Page 457 ~ Referral/Direct DOJ
Page 458 ~ Referral/Direct DOJ
Page 459 ~ Referral/Direct DOJ
Page 460 ~ Referral/Direct DOJ
Page 461 ~ Referral/Direct DOJ
Page 462 ~ Referral/Direct DOJ
Page 463 ~ Referral/Direct DOJ
Page 464 ~ Referral/Direct DOJ
Page 465 ~ Referral/Direct DOJ
Page 466 ~ Referral/Direct DOJ
Page 467 ~ Referral/Direct DOJ
Page 468 ~ Referral/Direct DOJ
Page 469 ~ Referral/Direct DOJ
Page 470 ~ Referral/Direct DOJ

Page 471 ~ Referral/Direct DOJ
Page 472 ~ Referral/Direct DOJ
Page 473 ~ Referral/Direct DOJ
Page 474 ~ Referral/Direct DOJ
Page 475 ~ Referral/Direct DOJ
Page 476 ~ Referral/Direct DOJ
Page 477 ~ Referral/Direct DOJ
Page 478 ~ Referral/Direct DOJ
Page 479 ~ Referral/Direct DOJ
Page 480 ~ Referral/Direct DOJ
Page 481 ~ Referral/Direct DOJ
Page 482 ~ Referral/Direct DOJ
Page 483 ~ Referral/Direct DOJ
Page 484 ~ Referral/Direct DOJ
Page 485 ~ Referral/Direct DOJ
Page 486 ~ Referral/Direct DOJ
Page 487 ~ Referral/Direct DOJ
Page 488 ~ Referral/Direct DOJ
Page 489 ~ Referral/Direct DOJ
Page 490 ~ Referral/Direct DOJ
Page 491 ~ Referral/Direct DOJ
Page 492 ~ Referral/Direct DOJ
Page 493 ~ Referral/Direct DOJ
Page 494 ~ Referral/Direct DOJ
Page 495 ~ Referral/Direct DOJ
Page 496 ~ Referral/Direct DOJ
Page 497 ~ Referral/Direct DOJ
Page 498 ~ Referral/Direct DOJ
Page 499 ~ Referral/Direct DOJ
Page 500 ~ Referral/Direct DOJ
Page 501 ~ Referral/Direct DOJ
Page 502 ~ Referral/Direct DOJ
Page 503 ~ Referral/Direct DOJ
Page 504 ~ Referral/Direct DOJ
Page 505 ~ Referral/Direct DOJ
Page 506 ~ Referral/Direct DOJ
Page 507 ~ Referral/Direct DOJ
Page 508 ~ Referral/Direct DOJ
Page 509 ~ Referral/Direct DOJ
Page 510 ~ Referral/Direct DOJ
Page 511 ~ Referral/Direct DOJ
Page 512 ~ Referral/Direct DOJ
Page 513 ~ Referral/Direct DOJ
Page 514 ~ Referral/Direct DOJ
Page 515 ~ Referral/Direct DOJ
Page 516 ~ Referral/Direct DOJ
Page 517 ~ Referral/Direct DOJ
Page 518 ~ Referral/Direct DOJ
Page 519 ~ Referral/Direct DOJ